Recovering Valuations on Demushkin Fields

Jochen Koenigsmann and Kristian Strømmen*

June 22, 2015

Abstract

Let K be a field with $G_K(2) \simeq G_{\mathbb{Q}_2}(2)$, where $G_F(2)$ denotes the maximal pro-2 quotient of the absolute Galois group of a field F. We prove that then K admits a (non-trivial) valuation v which is 2-henselian and has residue field $\mathbb{F}_2$. Furthermore, $v(2)$ is a minimal positive element in the value group Γ_v and $[\Gamma_v : 2\Gamma_v] = 2$. This forms the first positive result on a more general conjecture about the structure of pro-p Galois groups. As an application, we prove a strong version of the birational section conjecture for smooth, complete curves X over $\mathbb{Q}_2$, as well as an analogue for varieties.

1 Introduction

One of the most fruitful philosophies of modern number theory has been that one can understand the arithmetic of a field K by understanding the structure of the absolute Galois group $G_K = Gal(K^{sep}/K)$, where K^{sep} is a separable closure of K. If K_1 and K_2 are algebraic number fields, one has the celebrated Neukirch-Uchida Theorem which states that if $G_{K_1} \simeq G_{K_2}$ then $K_1 \simeq K_2$. A similar result for p-adic local fields was obtained by Mochizuki in [12], provided one adds some minimal extra structure on the Galois group.

*The second author was supported by an EPSRC Studentship at Oxford University, Award Number MATH1115.

2010 Mathematics Subject Classification. Primary 12J10, 11S20. Secondary 11G25

Keywords— Valuation theory, pro-p Galois groups, anabelian geometry, section conjecture, p-adics, Demushkin groups.

More generally, one could ask what structure of an *abstract* field is determined by its absolute Galois group. It is well known (by work of Artin-Schreier et. al.) that a field K is real-closed if and only if $G_K \simeq G_F$, where F is a real-closed field. The equivalent result for p-adically closed fields was obtained in [6]. In particular, $G_K \simeq G_{\mathbb{Q}_p}$ iff K is elementarily equivalent to $\mathbb{Q}_p$ in the language of rings. This was used in [8] to give a proof of the section conjecture in birational anabelian geometry for p-adic fields. In both cases the idea is to show that the abstract structure of the Galois group encodes the existence of an ordering (resp. a henselian valuation), and the existence of the ordering (resp. valuation) determines the arithmetic of the field.

One may reasonably follow up by asking if it suffices to consider smaller quotients of G_K. Of particular interest are the maximal pro-l quotients $G_K(l)$ of G_K, since for p-adic fields these quotients are well understood. Indeed, if ζ_l is a primitive l-th root of unity, $l \neq p$, then $G_{\mathbb{Q}_p(\zeta_l)}(l) \simeq \mathbb{Z}_l \rtimes \mathbb{Z}_l$ via the action of the cyclotomic character. Conversely, it is shown in [7] that if K is a field containing ζ_l and $G_K(l) \simeq \mathbb{Z}_l \rtimes \mathbb{Z}_l$, then K admits a non-trivial l-henselian valuation[1] with residue field of characteristic different from l. The valuation is recovered using the theory of 'rigid elements' (see e.g. [3], Section 2.2.3) via a combinatorial argument. The existence of suitable rigid elements is in turn inferred from the structure of $G_K(l)$, which implies that K satisfies a form of 'local reciprocity' in the form of a bijection between extensions of degree l and subgroups of $K^\times$ of index l given by the norm map.

The case $l \neq p$ lives in the 'tamely ramified' part of the Galois group. Much more mysterious is the 'wild' case $l = p$. Here the structure of $G_{\mathbb{Q}_p(\zeta_p)}(p)$ is known by work of Demushkin, Labute and Serre (cf. [20], 5.6). It is an example of a pro-p Demushkin group given by generators and relations which can be specified (see section 2): the same is true for any finite extension of $\mathbb{Q}_p$ containing ζ_p, and these fields are therefore canonical examples of what we call *Demushkin fields* (see Section 2.2). Taking into account that different extensions of $\mathbb{Q}_p$ can have the same pro-p Galois group[2], we have the following conjecture:

Conjecture 1. *Let $F/\mathbb{Q}_p$ be a finite extension, K an arbitrary field, where both F and K contain ζ_p. Suppose $G_F(p) \simeq G_K(p)$. Then there exists a non-trivial valuation v on K such that for some finite extension $F'/\mathbb{Q}_p$ with*

[1]For the definition of l-henselianity, l a prime, see Section 2.

[2]See Remark 2.8

$G_{F'}(p) \simeq G_F(p)$ and p-adic valuation w, the following holds:

- v is *p-henselian*
- $F'w = Kv$
- $[\Gamma_v : p\Gamma_v] = p$
- *There is a uniformizer π of (F', w) such that $\pi \in K \cap \overline{\mathbb{Q}}$ and $v(\pi)$ is a minimal positive element in Γ_v (in particular, the valuation is discrete).*[3]

Thus conjecturally, the 'wild' part of G_K sees a lot more of the structure of the field than the 'tame' part. In fact, in accordance with the Elementary Type Conjecture (see e.g. the introduction of [5] as well as [1]), it is expected that the following conjecture holds:

Conjecture 2. *Suppose $G_K(p)$ is a finitely generated pro-p Demushkin group of rank ≥ 3. Then there is a finite extension $F/\mathbb{Q}_p$ containing ζ_p such that $G_K(p) \simeq G_F(p)$.*

That is, one expects that essentially the only examples of finitely generated pro-p Galois groups which are Demushkin are the ones coming from finite extensions of $\mathbb{Q}_p(\zeta_p)$, and that the structure implied by being Demushkin is already enough to force the existence of a valuation which is as close to being p-adic as one could reasonably hope. This would be a major step in the programme of classifying all finitely generated pro-p Galois groups (see e.g. [1]).

Remark 1.1. Observe that in Conjecture 1, one should not expect the valuation to be rank 1, since e.g. $\mathbb{Q}_p(\!(\mathbb{Q})\!)$ has absolute Galois group isomorphic to that of $\mathbb{Q}_p$, and the associated valuation has higher rank.

The purpose of this article is to prove the following result (Theorem 4.15 in this paper), which constitutes the first positive result on these conjectures (though see [2] for some conditional results):

[3]Here Kv and Γ_v denote the residue field and value group of the valuation respectively.

Theorem 1. *Conjecture 1 is true in the case $F = \mathbb{Q}_2$. That is, if K is any field with $G_K(2) \simeq G_{\mathbb{Q}_2}(2)$, then there exists a non-trivial 2-henselian valuation v on K such that the residue field Kv is $\mathbb{F}_2$, the value group Γ_v is discrete with $v(2)$ a minimal positive element and $[\Gamma_v : 2\Gamma_v] = 2$.*

The proof hinges on the fact that any field K for which $G_K(p)$ is Demushkin satisfies a 'local reciprocity' law induced by the norm map (see Proposition 2.10), established in Section 2. The proof then proceeds in three steps. First, one uses the explicit structure of $G_{\mathbb{Q}_2}(2)$ to make some preliminary observations about $K^\times/(K^\times)^2$, which in turn imply that $char(K) = 0$. Secondly, putting $k = K \cap \overline{\mathbb{Q}}$, we show using class field theory that except in one exceptional case, k embeds into $\mathbb{Q}_2 \cap \overline{\mathbb{Q}}$ and hence that $K^\times/(K^\times)^2$ is generated as an $\mathbb{F}_2$-vector space by $-1, 2$ and 5. Assuming that we are not in the exceptional case, a consequence of this and 'local reciprocity' is that the 'lattice' of norm subgroups $Norm(K(\sqrt{a})^\times) \leqslant K^\times$ for $a \in K \setminus K^2$ is identical to that of $\mathbb{Q}_2$. Thirdly, we use an adaptation of the rigid element method to construct a valuation ring which satisfies all the desired properties. The fact that our construction yields a valuation ring depends on checking that certain elements in K are elements of certain norm subgroups. It turns out that this depends purely on the 'combinatorics' of the lattice of norm subgroups. Therefore, the existence of the desired valuation ring is lifted from k to K. This part is still quite mysterious: we cannot yet provide a good argument for why it works other than by direct calculations. Many of these calculations are relegated to the appendices to aid exposition. Finally, we show that the exceptional case simply cannot occur. This is done by showing that in this case, k admits a p-adic valuation for $p \neq 2$. Another application of the technique of norm-combinatorics allows us to lift this to a p-adic valuation on K, which is encoded in $G_K(2)$ by one of the main results from [7]. The fact that $\mathbb{Q}_2$ doesn't admit such a valuation allows us thereby to obtain the desired contradiction.

We do not currently have any ideas for how to prove Conjecture 2, though see [2] for connections between Conjecture 1 and 2.

Let us remark that there is no *conceptual* obstruction to carrying out a similar proof in cases where $p > 2$. However, in its current state, the method of proof relies heavily on explicit computations, which quickly become intractable for fields like $\mathbb{Q}_p(\zeta_p)$ with $p > 2$.

Finally, as an application, in Section 5 we show that Theorem 1 has the

following corollary, which gives a significant strengthening of the birational section conjecture (see [8]) over $\mathbb{Q}_2$.

Corollary 1. *Suppose X is a smooth, complete curve over $K = \mathbb{Q}_2$. Then every group-theoretic section of the exact sequence*

$$1 \to G_{\overline{K}(X)}(2) \to G_{K(X)}(2) \to G_K(2) \to 1$$

is induced by a unique rational point[4] *$a \in X(K)$, where $K(X)$ is the function field of X and $\overline{K}(X) = \overline{K} \otimes_K K(X)$.*

In fact, by more closely analysing the proof of the main theorem, we show that one can get away with an even smaller quotient of the Galois group, the so-called maximal $\mathbb{Z}/p$ elementary meta-abelian quotient (see the introduction to [15]). Thus we recover as a consequence of our work the main result of [15] in the case where the base field is $\mathbb{Q}_2$. We also prove a statement for varieties, strengthening the main result of [21].

2 Preliminaries

We collect some technical definitions and results used in the proof.

2.1 p-Henselianity

Given a valuation v on a field K, we let Kv denote the residue field and Γ_v the value group. The valuation ring will be denoted by $\mathcal{O}_v$. For all the results on valuations required in this paper, one can refer to [3]. However, we will remind the reader of the following

Definition 2.1. For a field K and a prime p, we write $K(p)$ for the **maximal pro-p Galois extension of** K, i.e., the compositum of all finite Galois extensions of K of order a power of p.

If v is a valuation on K, we say v is **p-henselian** if v has a unique extension to $K(p)$, or, equivalently, if Hensel's lemma holds for polynomials that split in $K(p)$.

Fact 2.2. *A field (K, v) is p-henselian if and only if v extends uniquely to every Galois extension of degree p.*

[4] See Section 5 for the precise meaning of this.

2.2 Demushkin Fields and the 'Local Reciprocity Law'

We start by recalling some basic facts about Demushkin groups and Brauer groups. For a reference on this and more see e.g. [20], [10] and [4].

Definition 2.3. Let G be a finitely generated pro-p group for some prime p. We say G is **Demushkin** if

(i) $dim_{\mathbb{F}_p}(H^1(G, \mathbb{Z}/p\mathbb{Z})) = n < \infty$

(ii) $dim_{\mathbb{F}_p}(H^2(G, \mathbb{Z}/p\mathbb{Z})) = 1$

(iii) The cup product $H^1(G, \mathbb{Z}/p\mathbb{Z}) \times H^1(G, \mathbb{Z}/p\mathbb{Z}) \to \mathbb{Z}/p\mathbb{Z}$ is a *non-degenerate* bilinear pairing.

The number $n = dim_{\mathbb{F}_p}(H^1(G, \mathbb{Z}/p\mathbb{Z}))$ is the rank of G, i.e., the minimal number of topological generators of G as a pro-p group.

Definition 2.4. Let p be prime. For a field F and $a \in F^\times \setminus (F^\times)^p$, define

$$N_F(a) := Norm_{F(\sqrt[p]{a})/F}(F(\sqrt[p]{a})^\times)$$

Since $F(\sqrt[p]{a}) = F(\sqrt[p]{b})$ whenever $a/b \in (F^\times)^p$, we will by abuse of notation also write $N_F(a)$ for $a \in F^\times/(F^\times)^p$, with a denoting both an element of $F^\times$ and its class modulo p-th powers.

Remark 2.5. If the base-field in question is clear, we will just write $N(a)$ for ease of notation.

Definition 2.6. Let K be a field containing ζ_p. We say that K is a **Demushkin field** whenever $G_K(p)$ is a Demushkin group.

Examples of Demushkin fields are finite extensions K of $\mathbb{Q}_p$ containing ζ_p ([20], 5.6). In this case, the structure of $G_K(p)$ is known: it is generated by $N + 2$ elements subject to a single relation r. Here $N = [K : \mathbb{Q}_p]$ and the relation r can be specified (see below).

Kummer Theory provides an isomorphism

$$H^1(G_K(p), \mathbb{Z}/p\mathbb{Z}) \simeq K^\times/(K^\times)^p$$

and the theory of Brauer groups gives

$$H^2(G_K(p), \mathbb{Z}/p\mathbb{Z}) \simeq {}_pBr(K) \simeq \mathbb{Z}/p\mathbb{Z}$$

where ${}_pBr(K)$ is the p-torsion subgroup of the Brauer group of K. The cup-product pairing can be identified with the Hilbert symbol

$$K^\times/(K^\times)^p \times K^\times/(K^\times)^p \to \mathbb{Z}/p\mathbb{Z}$$

sending the pair a, b to the symbol $(a, b)_K$ representing the central simple K-algebra with generators x, y subject to the relations $x^p = a, y^p = b, xy = \zeta_p yx$. We have $(a, b)_K = 1$ iff $a \in N(b)$ iff $b \in N(a)$.

If we denote by p^s the maximal power of p such that $\zeta_{p^s} \in K$, then one can pick generators $x_1, \ldots, x_{N+2}$ such that

$$r = x_1^{p^s}[x_1, x_2]...[x_{N+1}, x_{N+2}]$$

if $p^s \neq 2$ and N is even, where $x_1^{p^s}$ is defined to be 1 if $s = \infty$. If $p^s = 2$ and N is odd,

$$r = x_1^2 x_2^4 [x_2, x_3][x_4, x_5] \ldots [x_{N+1}, x_{N+2}]$$

where $[a, b]$ denotes the commutator. Passing to the abelianization it is not hard to see the following:

Fact 2.7. *Let F be a finite extension of $\mathbb{Q}_p$ containing ζ_p, with N and s as above. If $p^s \neq 2$, or $p^s = 2, N = 1$ (i.e., $F = \mathbb{Q}_2$), then*

$$G_F(p)^{ab} \simeq \mathbb{Z}/p^s\mathbb{Z} \times \mathbb{Z}_p^{N+1}$$

Remark 2.8. Since the isomorphism type of $G_K(p)$ is determined entirely by the integers N and s, we see that for example $\mathbb{Q}_2(\sqrt{2})$ and $\mathbb{Q}_2(\sqrt{5})$ have the same pro-2 Galois groups, as neither extension adds any new 2^k-th roots of unity.

Remark 2.9. Note that if $F = \mathbb{Q}_p(\zeta_p)$, then if F' is an arbitrary finite extension of $\mathbb{Q}_p$ containing ζ_p, we have $G_{F'}(p) \simeq G_F(p)$ if and only if $F = F'$, as F is the only such extension with Demushkin invariants $N = p + 1, s = 1$. Therefore in this case, F' may be taken to be F in the statement of Conjecture 1.

The crucial fact about Demushkin fields which we use is that they satisfy the following form of 'local reciprocity law'. The statement and proof here are due to Frohn and can be found in her thesis [4]. For the convenience of the reader we reproduce the proof here.

Proposition 2.10. *('Local Reciprocity') Let K be a Demushkin field with respect to p. Then for each $a \in K^\times \setminus (K^\times)^p$, $N(a)$ is a subgroup of $K^\times$ of index p, and the map*

$$\phi : \{K(\sqrt[p]{a}) : a \in K^\times \setminus (K^\times)^p\} \to \{H \leq K^\times/(K^\times)^p : H \text{ has index } p\}$$

given by $K(\sqrt[p]{a}) \mapsto N(a)$ is a bijection between Galois extensions of degree p and subgroups of $K^\times/(K^\times)^p$ of index p. Conversely, any field K containing ζ_p for which ϕ is a bijection is necessarily Demushkin.

Proof. Let us first prove that if K is Demushkin, then ϕ is a bijection.

Fix $a \in K^\times \setminus (K^\times)^p$. The induced map

$$\begin{aligned} K^\times/(K^\times)^p &\to \mathbb{Z}/p\mathbb{Z} \\ b &\mapsto (a, b) \end{aligned}$$

is surjective by virtue of the pairing being non-degenerate. Its kernel $N(a)$ is thus a subgroup of index p.

For any finite dimensional vector space, the number of subspaces of dimension 1 equals the number of subspaces of codimension 1. Since $K^\times/(K^\times)^p$ has finite $\mathbb{F}_p$-dimension by virtue of K being Demushkin, and one-dimensional subspaces of $K^\times/(K^\times)^p$ correspond to extensions of K of degree p, we have

$$|\{K(\sqrt[p]{a}) : a \in K^\times \setminus (K^\times)^p\}| = |\{H \leq K^\times/(K^\times)^p : \text{H has index p}\}| < \infty$$

Thus it suffices to show ϕ is injective. So let $a, b \in K^\times \setminus (K^\times)^p$ and suppose $N(a) = N(b)$. Since the pairing is non-degenerate, we may pick $x \in K^\times/(K^\times)^p$ such that (a, x) is non-trivial, and therefore generates $(\mathbb{Z}/p\mathbb{Z})^\times$. So $(a^n, x) = (b, x)$ for some n coprime to p. Now let $y \in K^\times/(K^\times)^p$ be arbitrary, with $(a, x)^m = (a, y)$. Then

$$(a, x^m y^{-1}) = 1$$

which implies $x^m = sy$ with $s \in N(a) = N(b)$. A simple calculation using bilinearity of the Hilbert symbol shows that $(a^n b^{-1}, y) = 1$. Since this is true

for every y, non-degeneracy again implies that $a^n = b$ in $K^\times/(K^\times)^p$, whence they generate the same extension of K, as desired.

For the converse, suppose $\zeta_p \in K$ and that ϕ is a bijection. In particular, the norm groups $N(a)$ have index p in $K^\times/(K^\times)^2$ and are therefore all *proper* subgroups. Thus the pairing is non-degenerate. Since $G_K(p)$ is assumed finitely generated, $\dim_{\mathbb{F}_p} H^1(G_K(p), \mathbb{Z}/p\mathbb{Z}) < \infty$. It remains therefore only to show that $H^2(G_K(p), \mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$. Let $(a,b) \in {}_pBr(K)$ be non-trivial. It suffices to show that $(x,b) = (a,b)^k$ for some k, for any x such that $(x,b) \neq 1$. For then if $(c,d) \in {}_pBr(K)$ is arbitrary, we simply pick $x \in K^\times \setminus (N(b) \cup N(c))$: then (x,b) and (x,c) are non-trivial, and $(c,d) = (c,x)^i = (b,x)^{ij} = (a,b)^{ijk}$ for some i,j,k, whence (a,b) is a generator of order p. But if (a,b) is non-trivial and $x \notin N(b)$, then $x \in b^k N(a)$ for some k, since $1, b, \ldots, b^{p-1}$ are coset representatives for $K^\times/N(a)$. But then it is easy to see that $(a,b)^k = (a,b^k) = (a,x)$, so we are done. □

Remark 2.11. In the case $p = 2$, we get from this that $N(a) = N(b)$ if and only if a and b are *equal* modulo squares. This will be crucially exploited in what follows.

3 The structure of $K^\times/(K^\times)^2$

For the rest of the paper we now fix once and for all a field K with

$$G_K(2) \simeq G_{\mathbb{Q}_2}(2).$$

Definition 3.1. For any field L, and a prime p, let

$$q_p(L) := dim_{\mathbb{F}_p} L^\times/(L^\times)^p.$$

For $x, y \in L^\times$, we write $x \sim y$ if the classes of x and y in $L^\times/(L^\times)^p$ are the same, i.e., if $x/y \in (L^\times)^p$. If $x_1, \ldots, x_n \in L^\times$, we write

$$\langle x_1, \ldots, x_n \rangle$$

for the subspace of $L^\times/(L^\times)^p$ generated by $x_1(L^\times)^p, \ldots, x_n(L^\times)^p$. So as a multiplicative group, $\langle x_1, \ldots, x_n \rangle$ is generated by the various products $x_{i_1} \ldots x_{i_k}$ and their powers.

In this section we aim to prove that the structure of $K^\times/(K^\times)^2$ is essentially the same as that of $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$. Let us first recall the structure of the latter group.

Proposition 3.2. *The group $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ has dimension $q_2(\mathbb{Q}_2) = 3$. A basis is given by the square classes of $-1, 2$ and 5. Hence $\mathbb{Q}_2^\times = \{\pm 1, \pm 2, \pm 5, \pm 10\}$ modulo squares.*

Proof. See e.g. [19] Chapter 2. □

We will show that the same is true for $K^\times/(K^\times)^2$. Indeed, we will show the stronger statement that any relation between square classes of *algebraic* elements in $\mathbb{Q}_2$ also holds in K. For example, in $\mathbb{Q}_2$, it is true that $3 = -5$ modulo squares, so the same will also hold in K. This will be made precise in Proposition 3.10 below.

First observe that by Kummer Theory, we have isomorphisms of $\mathbb{F}_2$-vector spaces

$$K^\times/(K^\times)^2 \simeq Hom(G_K(2), \mathbb{Z}/2\mathbb{Z}) \simeq Hom(G_{\mathbb{Q}_2}(2), \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$$

and hence $q_2(K) = q_2(\mathbb{Q}_2) = 3$.

Let us now show that -1 and 2 are independent, non-trivial square classes in $K^\times/(K^\times)^2$.

Lemma 3.3. *(i) There is a quadratic extension of $\mathbb{Q}_2$ which does not embed into a $\mathbb{Z}/4\mathbb{Z}$-extension of $\mathbb{Q}_2$, i.e., a Galois extension $L/\mathbb{Q}_2$ with Galois group $Gal(L/\mathbb{Q}_2) \simeq \mathbb{Z}/4\mathbb{Z}$.*

(ii) The extension $\mathbb{Q}_2(\sqrt{-1})$ admits a quadratic extension which does not embed into a $\mathbb{Z}/8\mathbb{Z}$-extension.

Proof. By Fact 2.7,

$$G_{\mathbb{Q}_2}(2)^{ab} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^2$$

and

$$G_{\mathbb{Q}_2(\sqrt{-1})}(2)^{ab} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}_2^3$$

from which one may readily deduce both claims, noting that $\mathbb{Q}_2(\sqrt{-1})$ does not contain a primitive 8th root of unity. □

Lemma 3.4. *(i) The characteristic of K is not 2, and $-1 \notin K^2$. In particular, $2 \in K^\times$.*

(ii) $2 \notin K(\sqrt{-1})^2$

(iii) -1 *is not the sum of two squares, and char(*K*)=0.*

Proof. The property (i) in the previous lemma is evidently equivalent to a statement about $G_{\mathbb{Q}_2}(2)$, and hence the statement is also true of K. But if char(K)=2, or $\sqrt{-1} \in K$, then every (separable) quadratic extension embeds into a $\mathbb{Z}/4\mathbb{Z}$-extension. In particular 2 is non-zero in K.

For (ii), note that $1/\sqrt{2} + i/\sqrt{2}$ is a primitive 8th root of unity. If such a root were to be found in $K(\sqrt{-1})$ then every $\mathbb{Z}/2\mathbb{Z}$-extension of $K(\sqrt{-1})$ would be embeddable into a $\mathbb{Z}/8\mathbb{Z}$-extension. But as above, this is not the case for K, since it is not the case for $\mathbb{Q}_2$ by (ii) of the previous lemma.

For (iii), note that by (ii), it follows that -1 and 2 are independent and non-trivial square classes in $K^\times/(K^\times)^2$. If -1 were a sum of two squares, that is, if $-1 \in N(-1)$, then since $2 \in N(-1)$ also, $N(-1) = \langle -1, 2\rangle$. So $-2 \in N(-1)$ whence $-1 \in N(-2)$, and so $N(-2) = \langle -1, 2\rangle = N(-1)$. By Proposition 2.10 and Remark 2.8, 2 is a square: contradiction.

In particular, since in any finite field, -1 is a sum of two squares, the characteristic of K must be 0. □

By the above lemma, we may now define the field $k := K \cap \overline{\mathbb{Q}}$. That is, k is the relative algebraic closure of $\mathbb{Q}$ in K. Our next goal is to elucidate the structure of k, and show that except for one 'bad case', k admits a '2-adic' valuation, i.e., a valuation such that the henselization k^h of k is isomorphic to $\mathbb{Q}_2 \cap \overline{\mathbb{Q}}$. Note that this latter field can be identified with the henselization $\mathbb{Q}^h$ of $\mathbb{Q}$ with respect to the 2-adic valuation, and is elementarily equivalent to $\mathbb{Q}_2$ (c.f. e.g [17]). In particular, k is a subfield of $\mathbb{Q}_2 \cap \overline{\mathbb{Q}}$.

Before proceeding with the next proposition, let us recall some results about extensions of p-adic fields.

Lemma 3.5. *Let* $L/\mathbb{Q}_p$ *be an extension containing a primitive* p*-th root of unity* ζ_p*.*

(i) If the extension is finite, then $q_p(L) = [L : \mathbb{Q}_p] + 2$

(ii) If p^∞ *divides* $[L : \mathbb{Q}_p]$*, then* ${}_pBr(L) = 0$*.*

Both statements are also true if we replace $\mathbb{Q}_p$ *with* $\mathbb{Q}^h$*, the henselization of* $\mathbb{Q}$ *with respect to the p-adic valuation.*[5]

[5]This is an example of the well known slogan that as far as algebra is concerned, henselizations are as good as completions.

Proof. See e.g. [20], 5.6, Lemma 3 and Theorem 4, for proofs of (i) and (ii).

Now let us consider both statements with completions replaced by henselizations. First consider (i), so $L/\mathbb{Q}^h$ is a finite extension and L contains ζ_p. Then, by virtue of being henselian, $[L : \mathbb{Q}^h] = [\hat{L} : \mathbb{Q}_p]$, where $\hat{L}$ denotes the completion (this follows e.g. from [13] Chapter 2, Corollary 8.4). But we also have $q_p(L) = q_p(\hat{L})$. Indeed, L (resp. $\mathbb{Q}^h$) is elementarily equivalent to $\hat{L}$ (resp. $\mathbb{Q}_p$), by virtue of being p-adically closed (see e.g. [17]). Hence the two fields satisfy all the same algebraic identities. In particular they must have the same number of inequivalent square classes. This implies the formula (i) for $L/\mathbb{Q}^h$.

For (ii), again, if $p^\infty \mid [L : \mathbb{Q}^h]$, then for every n we can find a finite subextension $F/\mathbb{Q}^h$ of L with $p^n \mid [F : \mathbb{Q}^h]$. Then $p^n \mid [F\mathbb{Q}_p : \mathbb{Q}_p]$ with $F\mathbb{Q}_p$ a finite subextension of $\tilde{L} := L\mathbb{Q}_p$. Hence ${}_pBr(\tilde{L}) = 0$. We want to show that also ${}_pBr(L) = 0$.

By the Merkurjev-Suslin Theorem ([11]), ${}_pBr(L)$ is generated by the cyclic algebras $(a, b)_L$. Therefore it suffices to show that $(a, b)_L = 1$ for any $a, b \in L$. We know that $(a, b)_{\tilde{L}} = 1$. Let $\tilde{F}$ be the extension of $\mathbb{Q}_p$ generated by a, b and the coefficients of a solution in $\tilde{L}$ to the equation $b = Norm_{\tilde{L}(\sqrt[p]{a})}(x)$, where $x \in \tilde{L}(\sqrt[p]{a})$. Then $(a, b)_{\tilde{F}} = 1$ by construction. But now $\tilde{F}$ is a *finite* extension of $\mathbb{Q}_p$, and hence is elementarily equivalent to $F := \tilde{F} \cap \overline{\mathbb{Q}} \subset L$. Since the statement $(a, b) = 1$ is equivalent to an existential sentence expressing b as a norm depending only on the parameter a, it follows that $(a, b)_F = 1$. Therefore ${}_pBr(L) = 1$. □

We will also require the following well known result of class field theory (see [13] Chapter 6, Corollary 4.5):

Theorem 3.6. *(Hasse Norm Theorem) Let L/F be a cyclic extension of number fields. Then for any $x \in F$, $x \in N(L)$ if and only if $x \in N(L_v)$ for every completion L_v/F_v.*

Remark 3.7. As with the above lemma, the statement is still true if we consider henselizations and real closures rather than completions, by similar reasoning.

We are now ready to characterize the structure of k. Let us begin with a basic observation.

Lemma 3.8. *Let $k = K \cap \overline{\mathbb{Q}}$. Then $q_2(k) = 3$.*

Proof. We have $q_2(k) \leq q_2(K) = 3$. Since -1 and 2 are independent in $k^\times/(k^\times)^2$, $q_2(k) = 2$ or 3. Suppose, for a contradiction, that $q_2(k) = 2$. Since $2 \in N_k(-1)$ is non-square, k is not Pythagorean. By [10] II. Proposition 5.1, this implies that the Witt ring $W(k) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. By Table 5.2 in [5], we find that $G_k(2) \simeq \mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$. Similarly one sees that $G_{k(i)}(2) \simeq \mathbb{Z}_2$, and so $q_2(k(i)) = 1$.

However, a simple calculation shows that since 2 is not a square in $k(i)$, neither is i. Further, $1+i$ and $i(1+i)$ both have norm 2, so i and $1+i$ are independent non-squares in $k(i)$, contradicting $q_2(k(i)) = 1$. □

We are now ready for the crucial lemma. Before stating the result, recall that a valuation v is called **tamely branching** at a prime p if the residue characteristic is not p, the value group Γ_v is not p-divisible, and if $[\Gamma_v : p\Gamma_v] = p$, then the residue field is not p-closed.

Lemma 3.9. *Given $k = K \cap \overline{\mathbb{Q}}$, one of the following cases holds:*

(A) The restriction map $G_K(2) \to G_k(2)$ is an isomorphism, and $k^h = \overline{\mathbb{Q}} \cap \mathbb{Q}_2$;

(B) $G_k(2)$ is the free pro-2 product $\mathbb{Z}/2\mathbb{Z} *_2 (\mathbb{Z}_2 \rtimes \mathbb{Z}_2)$, and k admits both an ordering and a p-adic valuation tamely branching at 2 with $p \equiv 5\,(8)$.

Proof. Choose any chain of number fields $k_0 = \mathbb{Q} \subseteq k_1 \subseteq \ldots \subset k$ such that $k = \bigcup_{i=0}^{\infty} k_i$. By Lemma 3.4, $-1 \notin N_K(-1)$, so also $-1 \notin N_k(-1)$ and $-1 \notin N_{k_i}(-1)$ for any i. If we let Σ_i denote the set of orderings and valuations v of k_i for which $-1 \notin N_{k_i^v}(-1)$, where k_i^v is a real-closure, resp. a henselization, of k_i with respect to v, then by the Hasse Norm Theorem every Σ_i is non-empty. For $i < j$, each valuation in Σ_j lies above a valuation in Σ_i. Now, it is easy to see that Σ_0 contains the archimedean valuation of $\mathbb{Q}$. Since it is only for $p = 2$ that the Hilbert symbol $(-1,-1)_p = -1$, we see that Σ_0 consists of exactly these two valuations, and hence every valuation in Σ_i lies above one of these. Since the Σ_i are finite and non-empty, their inverse limit Σ_∞ is non-empty, and every valuation $v \in \Sigma_\infty$ is either archimedean (corresponding to an ordering) or duadic. We now distinguish between two cases.

Case A: Suppose that Σ_∞ contains a duadic valuation v. If we let k^h denote the henselization of k with respect to v, then $-1 \notin N_{k^h}(-1)$. If we denote by $\mathbb{Q}^h$ a henselization of $\mathbb{Q}$ with respect to the 2-adic valuation (which we may without loss of generality take to be $\mathbb{Q}_2 \cap \overline{\mathbb{Q}}$) then there is a natural

embedding $\mathbb{Q}^h \hookrightarrow k^h$. Let $F := k^h$. We claim that the extension $F/\mathbb{Q}^h$ is finite.

Indeed, first notice that if 2^∞ divides $[F : \mathbb{Q}^h]$, then ${}_2Br(F) = 0$ by Lemma 3.6. But the Brauer group of F contains the non-trivial degree-two element $(-1,-1)$, so this cannot be the case. Therefore there is a finite extension $L/\mathbb{Q}^h$ such that F/L has odd, possibly infinite, degree. Since F/L is of odd degree, the canonical map

$$L^\times/(L^\times)^2 \to F^\times/(F^\times)^2 \tag{1}$$

is injective. By Lemma 3.6. (i),

$$q_2(L') = [L' : \mathbb{Q}^h] + 2 \tag{2}$$

for any finite subextension L'/L of F, so we see that $q_2(F) \geq q_2(L')$ by the injectivity of the map in (1). But now, because $\dim_{\mathbb{F}_2} F^\times/(F^\times)^2 \leq 3$, the degree $[F : L]$ must be finite. Hence, applying the rank-formula to $F/\mathbb{Q}^h$, we get

$$3 \geq q_2(F) = [F : \mathbb{Q}^h] + 2$$

giving $[F : \mathbb{Q}^h] = 1$. So $k \hookrightarrow k^h = \mathbb{Q}^h = \mathbb{Q}_2 \cap \overline{\mathbb{Q}}$.

Since $q_2(k) = 3$ (Lemma 3.8), and $-1, 2$ and 5 form a basis for ${\mathbb{Q}^h}^\times/({\mathbb{Q}^h}^\times)^2$, it follows that $-1, 2$ and 5 also form a basis for $k^\times/(k^\times)^2$. We also know that $-3/5$ is a square in k, since this is true in k^h; it follows that $-5 \in N(-2)$. Since $G_{k^h}(2)$ is Demushkin of rank 3, the norm groups of k are generated by exactly 2 elements. From this it is easy to work out all the norm groups $N_k(a)$ for $a \in \{-1, \pm 2, \pm 5, \pm 10\}$. They are as follows:

- $N_k(-1) = \langle 2, 5\rangle$
- $N_k(2) = \langle -1, 2\rangle$
- $N_k(5) = \langle -1, 5\rangle$
- $N_k(10) = \langle -1, 10\rangle$
- $N_k(-2) = \langle 2, -5\rangle$
- $N_k(-5) = \langle -2, 5\rangle$
- $N_k(-10) = \langle -2, -5\rangle$

It follows by Proposition 2.10 that k is Demushkin of rank 3. Hence $G_K(2)$ and $G_k(2)$ are Demushkin with the same invariants, and so are isomorphic finitely generated pro-2 groups. Thus the epimorphism $G_K(2) \to G_k(2)$ is an isomorphism, by the profinite pidgeon-hole principle (see [18] Proposition 2.5.2).

Case B: Suppose Σ_∞ does not contain a duadic valuation. Then k is formally real, and $k^\times/(k^\times)^2 = \langle -1, 2, c\rangle$ for some $c \in k^\times$. We know as before that the norm groups are generated by at most 2 elements. In particular, either $N_k(-1) = \langle 2\rangle$ or we can choose c such that $N_k(-1) = \langle 2, c\rangle$. Suppose, for a contradiction, that $N_k(-1) = \langle 2\rangle$. Since $N_k(-1) = \cap P$, where the intersection is over all positive cones P of distinct orderings of k, and $N_k(-1)$ has index 4 in $k^\times$, k must admit two distinct orderings. Each of these will prolong in two distinct ways to $k(\sqrt{2})$, which therefore admits 4 distinct orderings. Notice next that $1 + \frac{1}{\sqrt{2}}$ has norm $1/2$, hence is not a square, but is positive with respect to any ordering on $k(\sqrt{2})$. Hence $k(\sqrt{2})$ is not Pythagorean. It follows that $q_2(k(\sqrt{2})) \geq 5$. But one also has $q_2(K(\sqrt{2})) = q_2(\mathbb{Q}_2(\sqrt{2})) = 4$. This gives a contradiction, since $k(\sqrt{2})$ is relatively algebraically closed in $K(\sqrt{2})$.

We conclude that $N_k(-1) = \langle 2, c\rangle$, and k admits a unique ordering with positive cone $N_k(-1)$. Note that since $N_k(2) = \langle -1, 2\rangle$, $c \notin N_k(2)$. However, being positive, $c \in N_{k^r}(2)$, where k^r is the real closure of k. A similar argument as before therefore shows that the set of valuations Σ_∞^* for which $c \notin N_{k^h}(2)$ is non-empty, but does not contain a real place.

If Σ_∞^* contains a duadic valuation, we end up back in Case A and we are done. So suppose it does not. Then it must contain a p-adic valuation v for which $v(c)$ is not 2-divisible, and by choosing c such that $c = 1 + a^2$ for some $a \in k$, $v(c)$ is odd and positive. Furthermore, -1 is a square in the residue field, while 2 is not, and hence $p \equiv 5\,(8)$. It follows, for example by another computation of the Witt ring of k, that $G_k(2) \simeq \mathbb{Z}/2\mathbb{Z} *_2 (\mathbb{Z}_2 \rtimes \mathbb{Z}_2)$ with presentation $\langle a, b, c : a^2 = b^4[b, c] = 1\rangle$. Here $\mathbb{Z}/2\mathbb{Z} = G_{k^r}(2)$, and $\mathbb{Z}_2 \rtimes \mathbb{Z}_2 \simeq G_{k^h}(2)$, where k^r (resp. k^h) is the real closure (resp. henselization) of k. □

We will ultimately show that Case B above does not occur. However, we have as of yet not found a way to rule this out other than by applying the norm-combinatorics machinery developed in Section 4. Note that it suffices to obtain a contradiction in the case where $tr.deg_k(K) = 1$, since if we let $t \in K$ be transcendental over k, the relative algebraic closure of $k(t)$ in

K has the same pro-2 Galois group as K. For this reason we can show that a suitably generalized 'local-global' principle for Brauer groups as in [14] will rule out Case B. However, we have not yet been able to prove such a principle. Let us remark that a major source of difficulty is that, as remarked in the proof of Lemma 3.9, $G_k(2) \simeq \langle a, b, c : a^2 = b^4[b, c] = 1\rangle$ in Case B, and as an abstract group, this *does* in fact occur as a quotient of $G_K(2) \simeq \langle x, y, z : x^2y^4[y, z] = 1\rangle$. Therefore, Case B cannot be ruled out by purely group-theoretic reasons. As will be seen, our proof for ruling it out involves the arithmetic of the field in a subtle way.

Proposition 3.10. *Assume we are in Case A, that is, $k \subset \mathbb{Q}_2 \cap \overline{\mathbb{Q}}$. Then an $\mathbb{F}_2$-basis for $K^\times/(K^\times)^2$ is given by the classes of $-1, 2$ and 5. For any $q \in \overline{\mathbb{Q}}$, $q \sim 1$ in K if and only if $q \sim 1$ in $\mathbb{Q}_2$. The quadratic norm groups $N(a)$ of K are all as follows:*

- $N_K(-1) = \langle 2, 5\rangle$
- $N_K(2) = \langle -1, 2\rangle$
- $N_K(5) = \langle -1, 5\rangle$
- $N_K(10) = \langle -1, 10\rangle$
- $N_K(-2) = \langle 2, -5\rangle$
- $N_K(-5) = \langle -2, 5\rangle$
- $N_K(-10) = \langle -2, -5\rangle$

Proof. Since $-1, 2$ and 5 form a basis for $k^\times/(k^\times)^2$, they are independent modulo squares, and since $K^\times/(K^\times)^2$ has dimension 3, these also form a basis of $K^\times/(K^\times)^2$. The structure of the norm groups for K must be the same as that of k, since $K^\times/(K^\times)^2$ has the same basis as k and the norm groups have the same size. These were calculated in the proof of the above lemma, resulting in the above list. For the last part, note that $q \sim 1$ in K iff $q \sim 1$ in k, since if q were a non-square in k, it could only become a square in K if one of $\pm 1, \pm 2, \pm 5, \pm 10$ become square in k, which we know can't happen. Since k embeds into $\mathbb{Q}_2$, the same argument shows that $q \sim 1$ in k iff $q \sim 1$ in $\mathbb{Q}_2$. □

4 Construction of the Valuation: Norm Combinatorics

In $\mathbb{Q}_2$, we can detect the valuation ring via norms by the equality

$$Norm(\mathbb{Q}_2(\sqrt{5})^\times) = \mathbb{Z}_2^\times \cdot (\mathbb{Q}_2^\times)^2$$

which follows from the fact that $\mathbb{Q}_2(\sqrt{5})$ is the (unique) unramified quadratic extension of $\mathbb{Q}_2$. We will use this observation along with the following construction from the theory of 'rigid elements' (see e.g. [3], Section 2.2.3) to construct the valuation of Theorem 1. The general setup is as follows.

Let p be a rational prime, F a field, $T \leqslant F^\times$ a subgroup containing $(F^\times)^p$. Define the sets

$$\mathcal{O}_1(T) := \{x \in F \setminus T : 1 + x \in T\} \quad (3)$$
$$\mathcal{O}_2(T) := \{x \in T : x\mathcal{O}_1(T) \subseteq \mathcal{O}_1(T)\} \quad (4)$$

and

$$\mathcal{O}(T) := \mathcal{O}_1(T) \cup \mathcal{O}_2(T).$$

Lemma 4.1. *Suppose that for any $x, y \in \mathcal{O}_1(T)$, one has $1 - xy \in T$. Then $\mathcal{O}$ is a (non-trivial) valuation ring of F with $\mathcal{O}^\times \subset T$ and $\mathcal{O}_1 \cdot \mathcal{O}_1 \subset \mathcal{O}_2$.*

Proof. This is a straightforward adaptation of Theorem 2.2.7 and its proof in [3]. □

Case A

In this section we will always be working with a field K such that $G_K(2) \simeq G_{\mathbb{Q}_2}(2)$ and $k \subset \mathbb{Q}_2 \cap \overline{\mathbb{Q}}$.

Consider the above construction with $p = 2$, $F = K$ and $T = N(5)$. In this case we write $\mathcal{O}_1$ instead of $\mathcal{O}_1(T)$ etc. Notice that for $K = \mathbb{Q}_2$, the elements in $\mathcal{O}_1$ (other than 0) are those with positive, odd valuation, by the ultrametric inequality, and so $\mathcal{O}_2$ consists of the 2-adic integers with even valuation. Therefore in this case $\mathcal{O}$ is indeed just $\mathbb{Z}_2$. We will show that the condition of the lemma holds for our abstract K as well, and then deduce that the valuation ring $\mathcal{O}(N(5))$ satisfies the additional properties desired.

Remark 4.2. One may be tempted to use directly the statement in [3] Theorem 2.2.7 for $p = 2$. However, there appears to be no obvious way to exclude the possibility that the subgroup T_1 of $K^\times$ obtained for which $\mathcal{O}(T_1)$ is a valuation ring, is in fact the whole of $K^\times$. That is, there is no way of telling if the valuation obtained is trivial or not. To show that T_1 may be taken to be $N(5)$ (i.e., to show non-triviality), the only apparent strategy is to show directly that the specified condition holds.

The idea of the proof is to decompose the term $1 - xy$ in several ways, all of which are visibly in certain norm groups $N(a)$. Working on a case by case basis, depending on the square classes of $x, y, 1 + x$ and $1 + y$, this places $1 - xy$ in the intersection of several norm groups, which are known by Proposition 3.10. In all cases, the possible square classes of $1 - xy$ thus obtained are always in $N(5)$. As an intermediate step, we need to establish that $\pm 1, \pm 5$ and $\pm 1/5 \in \mathcal{O}_2$, i.e., that these numbers are 'units' in $\mathcal{O}$; of course we expect this to be true since these numbers are units in $\mathbb{Z}_2$. Doing this amounts to computing the square class of expressions $1+ax$ when $x \in \mathcal{O}_1$ and $a \in \{\pm 1, \pm 5, \pm 1/5\}$. This is again done by writing $1 + ax$ as a norm in several different ways, thereby severely restricting its possible square class.

The proof shows that the square class of expressions like $1+ax$, for $a \in k$, $x \in K$, is determined entirely by the square class of $x, 1 + x$ and the 'lattice' of norm-groups. If such a statement could be made rigorous and then proved, one could deduce that $\mathcal{O}(N(5))$ is a valuation ring simply because it is one for k. Unfortunately, such a structural proof still eludes us, and we instead resort to direct computations.

Remark 4.3. Notice that $0 \in \mathcal{O}_1(T)$ for any T. In the calculations and lemmas established in the following, we always ignore this case, as it can easily be seen that 0 will satisfy all the claims made, or that the resulting computation gives 0, which we know to be in $\mathcal{O}_1$.

Before we begin, let us for ease of exposition introduce some notation. For $a_i \in K^\times$, we write

$$\{a_1, a_2, \ldots, a_n\}$$

as shorthand for the subset

$$a_1(K^\times)^2 \cup a_2(K^\times)^2 \cup \ldots \cup a_n(K^\times)^2$$

of $K^\times$.

Our first lemma should be thought of as proving that $v(2) > 0$.

Lemma 4.4. *Let $x \in \mathcal{O}_1$. Then $1 + 2x$ and $1 + 4x$ are in $N(5)$.*

Proof. See Appendix A. The proof uses explicit calculations on a case by case basis, as explained above. □

Exploiting that $N(5)$ is closed under multiplication, the above lemma can be used to prove the crucial

Corollary 4.5. *$-1, 5$ and $1/5 \in \mathcal{O}_2$, and consequently so is -5 and $-1/5$.*

Proof. We need to show that if $x \in \mathcal{O}_1$, then also $-x, 5x$ and $x/5$ are in $\mathcal{O}_1$. That then also -5 and $-1/5$ are in $\mathcal{O}_2$ follows since $\mathcal{O}_2$ is clearly closed under multiplication.

If $x \in \mathcal{O}_1$, then[6] so is $-x/(1+x)$, and hence, by Lemma 4.4, $1 - 2x/(1 + x) \in N(5)$, whence $(1 + x)(1 - 2x/(1 + x)) = 1 - x \in N(5)$. So $-x \in \mathcal{O}_1$.

Next, for any $x \in \mathcal{O}_1, -x/(1 + x) \in \mathcal{O}_1$ and consequently so is $x/(1 + x)$ by the above. Thus, by Lemma 4.4, $1 + 4x/(1 + x) \in N(5)$, whence $(1 + x)(1 + 4x/(1 + x)) = 1 + 5x \in N(5)$. Hence $5x \in \mathcal{O}_1$.

Finally, if $x \in \mathcal{O}_1$, then $1 - 2/(1 + x) = -(1 - x)/(1 + x) \in N(5)$ so $-2/(1+x) \in \mathcal{O}_1$. Since we know already that $-1 \in \mathcal{O}_2$, we get $2/(1+x) \in \mathcal{O}_1$ and so $1 + 4/(1 + x) \in N(5)$, whence $(1 + 4/(1 + x))(1 + x) = 5 + x \in N(5)$, and so $1 + (1/5)x \in N(5)$. Hence $1/5 \in \mathcal{O}_2$. □

We are now ready to prove the critical

Proposition 4.6. *For any $x, y \in \mathcal{O}_1$, $1 - xy \in N(5)$.*

Proof. The key point is to note the following decompositions:

$$\begin{aligned}
1 - xy &= (1 + y)\left(1 + (1 + x)\frac{-y}{1 + y}\right) \\
&= (1 - y)\left(1 + (1 - x)\frac{y}{1 - y}\right) \\
&= (1 + 5y)\left(1 + (1 + 5^{-1}x)\frac{-5y}{1 + 5y}\right) \\
&= (1 - 5y)\left(1 + (1 - 5^{-1}x)\frac{5y}{1 - 5y}\right)
\end{aligned}$$

[6] Observe that $-x/(1 + x)$ is not in $N(5)$ and $1 - x/(1 + x) = 1/(1 + x) \in N(5)$.

Therefore, thanks to Corollary 4.5, it suffices to show for example that $1+(1+x)y' \in N(5)$, where $y' = -y/(1+y)$. Now one notes that $1+(1+x)y' = (1+x)+xy' = (1+x)(1+y')-y'$. Therefore if we know the square classes of $x, y, 1+x$ and $1+y$, this gives three different expressions of $1+(1+x)y'$ as a norm, severely limiting the possible square class of $1-xy$. By doing the same procedure for different choices of a decomposition of $1-xy$, one can show, case by case, that one always has $1-xy \in N(5)$. Since it is known that the expressions $1+ax$, $a \in \{\pm 1, \pm 5, \pm 5^{-1}\}$, are all in $N(5)$, it is straightforward to pin down their exact square class in many cases (see Appendix A), and this is used throughout.

This is all elementary, but tedious. The calculations may be found in Appendix A. We include one case here to exemplify the above remarks.

Suppose $x \sim -2, 1+x \sim 1, y \sim -2, 1+y \sim 1$. Then

$$1-xy \sim 1+(1+x)\frac{-y}{1+y} \in N(-2)$$

Also, one can quickly check that $1+5^{-1}x \sim 1, 1+5y \sim 1$. Indeed, $1+5^{-1}x \in N(10)$ so $5+x \in 5N(10)$. Also $5+x = (1+x)+4 \in N(-1)$, and since we also know $5+x \in N(5)$ by Corollary 4.5, we must have $5+x \sim 5$, so $1+5^{-1}x \sim 1$ as claimed. Similarly, $5(1+5^{-1}y) = (1+y)+4$. The first expression is visibly in $5N(10)$ while the second is visible in $N(-1)$. But also $5+y \in N(5)$ since $5 \in \mathcal{O}_2$. Hence $5+y \in N(5) \cap 5N(10) \cap N(-1) = \{5\}$. Hence $1+5^{-1}y \sim 1$.

It follows that

$$1-xy \sim 1+(1+5^{-1}x)\frac{-5y}{1+5y} \in N(-10)$$

Thus $1-xy \in N(-2) \cap N(-10) = \{1, -5\} \subset N(5)$ as desired. □

Corollary 4.7. *The set $\mathcal{O}$ is a non-trivial valuation ring of K with residue characteristic 2.*

Proof. Non-triviality is clear since $\mathcal{O}^\times \subset N(5)$. Also, since $2 \notin N(5)$, the value of 2 is strictly positive, whence 2 becomes trivial in the residue field. □

Remark 4.8. We will choose a valuation v with $\mathcal{O}_v = \mathcal{O}$, and denote the value group, maximal ideal and residue field of v as Γ, $\mathcal{M}$ and Kv respectively.

We now elucidate the structure of $\mathcal{O}_2$ further. Put

$$A := \{x \in N(5) : 1 + 2x \in N(5)\} \tag{5}$$

In $\mathbb{Q}_2$, this set coincides, by the ultrametric inequality, with the 2-adic integers with even valuation. Hence we expect the following

Lemma 4.9. $\mathcal{O}_2 = A$.

Proof. One direction is trivial: if $x \in \mathcal{O}_2$ then as $2 \in \mathcal{O}_1$, we have $2x \in \mathcal{O}_1$ so that $1 + 2x \in N(5)$. That is, $x \in A$.

For the other direction, note that if $x \in A$ then $2x \in \mathcal{O}_1$. Hence A is invariant under multiplication by $\pm 1, \pm 5$ and $\pm 5^{-1}$. Suppose therefore that we can prove that for any $x \in A$ with $x \sim 1$, that $x \in \mathcal{O}_2$. Then as $\mathcal{O}_2$ is also invariant under multiplication by those numbers, it easily follows that $x \in \mathcal{O}_2$ also when $x \sim -1$ or ± 5. Because $\mathcal{O}_2 \subset N(5) = \{\pm 1, \pm 5\}$, these are the only possible square classes of x. If $x \sim 1$, then in addition we know $1 + 2x \in N(5) \cap N(-2) = \{1, -5\}$. Thus we need only consider the following two cases:

- $\boxed{1 + 2x \sim 1}$ We need to show that for any $y \in \mathcal{O}_1$, $xy \in \mathcal{O}_1$. Since $\mathcal{O}_1$ is invariant under $\pm 1, \pm 5, \pm 5^{-1}$, as before, we can assume that $y \sim 2$, whence $1 - y \in N(5) \cap N(2) = \{\pm 1\}$.

  Suppose first $1 - y \sim 1$. Then if $1 + 2x = a^2$, we get $1 + 2xy = (1-y) + a^2 y \in N(-1) \cap N(-2)$. But it's also in $N(5)$ since $-2x, y \in \mathcal{O}_1$ whence $1 - (-2x)y \in N(5)$ by Proposition 4.6. So $1 + 2xy \sim 1$. Hence $1 + 5xy = (1 + 2xy) + 3xy \in N(-10) \cap N(10) = \{1, 10\}$, using that $3 \sim -5$. If $1 + 5xy \sim 10$, we get $1 + 4xy = (1 + 5xy) - xy \in 2N(5)$. But since $\mathcal{O}$ is a ring, $2xy \in \mathcal{O}_2$ and so $4xy \in \mathcal{O}_1$, whence $1 + 4xy \in N(5)$, contradiction. So $1 + 5xy \in N(5)$, whence it follows that $5xy \in \mathcal{O}_1$ and hence so is xy.

  Suppose now that $1 - y \sim -1$. Then $1 + 2xy \in N(2) \cap N(5) \cap N(-1) = \{1\}$. Arguing as above, $1 + 5xy \in N(5)$ and we're done also in this case.

- $\boxed{1 + 2x \sim -5}$ First suppose $y \sim 2, 1 - y \sim 1$. Then $1 + 2x = -5a^2$ for some a, whence $1 + 2xy = (1-y) - 5a^2 y$. Since $2x \in \mathcal{O}_1, 1 + 2xy \in N(5)$ as well. Consequently $1 + 2xy \in N(5) \cap N(-1) \cap N(10) = \{1\}$.

It follows that $1+xy = (1+2xy) - xy \in N(-2) \cap N(2) = \{1,2\}$. If $1+xy \sim 2$, then $1+4xy = (1+xy)+3xy \in 2N(5)$. But as $4xy \in \mathcal{O}_1$, $1+4xy \in N(5)$ as well, giving a contradiction. Hence $1+xy \sim 1$ and we're done.

Next suppose $y \sim 2, 1-y \sim -1$. Then as above, we get $1+2xy = (1-y)-5a^2y$ for some a, and so $1+2xy \in N(5) \cap -N(-10) \cap N(-1) = \{5\}$. Now $1+5xy = (1+2xy)+3xy \in 5N(2) \cap N(-10) = \{-5, 10\}$. If $1+5xy \sim 10$, then $1+4xy = (1+5xy) - xy \in -2N(5) \cap N(5)$ which is empty. Hence we must have $1+5xy \sim -5$. That is, $5xy \in \mathcal{O}_1$, so $xy \in \mathcal{O}_1$ as well.

□

Since $\mathcal{O}^\times \subset \mathcal{O}_2$, we have

Corollary 4.10. *The units are*

$$\mathcal{O}^\times = \{x \in N(5) : 1+2x \in N(5) \text{ and } 2+x \in N(5)\} \tag{6}$$

and the maximal ideal is the disjoint union $\mathcal{M} = \mathcal{O}_1 \sqcup B$ where

$$B := \{x \in N(5) : 1+2x \in N(5) \text{ and } 2+x \notin N(5)\} \tag{7}$$

Proposition 4.11. $B = 2\mathcal{O}_1$.

Proof. If $x \in B$, then as $2+x \notin N(5)$, $1+x/2 \in N(5)$, so $x/2 \in \mathcal{O}_1$, whence $x \in 2\mathcal{O}_1$. The other direction follows easily from the previous Lemma in a similar fashion. □

Proposition 4.12. $v(2)$ *is a minimal positive element in* Γ.

Proof. Since $\mathcal{O}_1 \subset \mathcal{M}$, $v(2) > 0$. Now suppose we have $x \in \mathcal{M}$ with $v(x) < v(2)$, i.e., $2/x \in \mathcal{M} = \mathcal{O}_1 \cup 2\mathcal{O}_1$. If $2/x \in 2\mathcal{O}_1$, then $x^{-1} \in \mathcal{O}_1$, contradicting $v(x) > 0$. If $2/x \in \mathcal{O}_1$, then it cannot be the case that $x \in \mathcal{O}_1$, or else $2 \in \mathcal{O}_1 \cdot \mathcal{O}_1 \subset \mathcal{O}_2$. Hence $x \in 2\mathcal{O}_1$, so $x = 2y, y \in \mathcal{O}_1$. Then $v(2) > v(x) = v(2y) > v(2)$, which is absurd. □

Since $v(2) > 0$, it is clear that Kv has characteristic 2. In fact, more detailed calculations show that the residue field is exactly $\mathbb{F}_2$.

Proposition 4.13. *If $x \in \mathcal{O}^\times$, then $1+x \in \mathcal{M}$. In particular, $\mathcal{O}/\mathcal{M}$ contains only two elements, so is $\mathbb{F}_2$.*

Proof. As usual, one proceeds on a case by case basis.

Suppose $x \in \mathcal{O}^\times$ with $x \sim 1$. Then we aim to show $1 + x \notin N(5)$ and so in particular is not a unit. Indeed, $1 + 2x \in N(5) \cap N(-2) = \{1, -5\}$ and $2 + x \in N(5) \cap N(-2)$ as well. Suppose $1 + 2x \sim 1$, equalling a^2 say. Then $2 + x = a^2/2 + 3/2$, and since $3 \sim -5$, this is in $2N(5)$, a contradiction.

So $1 + 2x \sim -5$, and a similar calculation shows $2 + x \in N(-1)$, so $2 + x \sim -5$.

Now $1 + x \in N(-1)$, so if it were also in $N(5)$, it would be equivalent to 1 or 5. But it is easy to check that both of these possibilities contradict $2 + x \sim -5$.

The other cases are similar. One shows either that $1 + x \notin N(5)$, or that $3 + x \notin N(5)$; the former implies $1 + x \in \mathcal{O}_1$, while the latter implies $1 + x \in 2\mathcal{O}_1$. The remaining cases may be found in Appendix B. □

Next, we would like to show 2-henselianity. We shall see that in our case, this property is inherited from the 2-henselianity of $k = K \cap \overline{\mathbb{Q}}$.

Proposition 4.14. *The valuation $\mathcal{O}$ is 2-henselian.*

Proof. It suffices to show that $\mathcal{O}$ extends uniquely to every quadratic extension of K. Recall that k^h can be identified with the henselization of $\mathbb{Q}$ with respect to the 2-adic valuation. Hence k^h is henselian, and the ramification indices and degrees with respect to the different quadratic extensions are known: we have $e = 1, f = 2$ for the extension $k^h(\sqrt{5})$, and $e = 2, f = 1$ for all the other extensions. Furthermore, note that both K and k^h have residue fields $\mathbb{F}_2$.

Hence if we let $\mathcal{O}'$ be any extension of $\mathcal{O}$ to $K(\sqrt{5})$, and let f' be the residue degree of the induced extension with respect to $k^h(\sqrt{5})/k^h$, we get, by multiplicativity of residue degrees, that $2 \geq f(\mathcal{O}'/\mathcal{O}) = 2f' \geq 2$, and hence $f(\mathcal{O}'/\mathcal{O}) = 2$.

For all the other quadratic extensions $L = K(\sqrt{a})$, we know that since $e(\mathcal{O}_L/\mathcal{O}) \leq 2$, we have that the index is either 2 or the value groups Γ_K and Γ_L are isomorphic. Let $k' = L \cap \overline{\mathbb{Q}} = k(\sqrt{a})$. Then since $\Gamma_{k^h} = \Gamma_K \cap \Gamma_{\overline{\mathbb{Q}}}$ and $\Gamma_{(k')^h} = \Gamma_L \cap \Gamma_{\overline{\mathbb{Q}}}$, it follows that if $\Gamma_K = \Gamma_L$, then $\Gamma_{k^h} = \Gamma_{(k')^h}$. Since for $a \not\sim 5$, the ramification index with respect to $(k')^h/k^h$ is always 2, it follows that it must also be 2 for L/K.

We have shown that for any quadratic extension of K, $ef = 2$ always holds, which implies by the fundamental inequality for valuations ([3] Theo-

rem 3.3.4) that there is always at most one extension of $\mathcal{O}$ to any such field. Hence the valuation is 2-henselian. □

In the next section we will show that Case B of Lemma 3.9 does not occur. Therefore upon combining the above results we obtain at last our main result.

Theorem 4.15. *Suppose $G_K(2) \simeq G_{\mathbb{Q}_2}(2)$. Then there is a valuation v on K which is 2-henselian, has discrete value group with $v(2)$ as a minimal positive element, residue field $\mathbb{F}_2$ and $[\Gamma : 2\Gamma] = 2$.*

Proof. The only thing remaining to prove is that $[\Gamma : 2\Gamma] = 2$. Note that $\Gamma \simeq K^\times/\mathcal{O}^\times$, and $\mathcal{O}^\times(K^\times)^2 = N(5)$. Since $v(\mathcal{O}^\times(K^\times)^2) = 2\Gamma$, and $N(5)$ has index 2 in $K^\times$, this implies that

$$\Gamma/2\Gamma \simeq \frac{K^\times}{\mathcal{O}^\times(K^\times)^2}$$

has order 2. □

In fact, upon reviewing the proof, we see that we didn't need all of $G_K(2)$, only the significantly smaller quotient $Gal(K''/K)$, where K'' is the so-called maximal $\mathbb{Z}/2\mathbb{Z}$ elementary meta-abelian extension of K. Indeed, Lemma 3.3 and 3.4 clearly only need this quotient, and it is well known (see e.g. [15]) that the Galois cohomology used is already seen by $Gal(K''/K)$. Therefore we get the much stronger

Corollary 4.16. *Suppose $Gal(K''/K) \simeq Gal(\mathbb{Q}_2''/\mathbb{Q}_2)$. Then the conclusion of Theorem 4.15 holds.*

Case B

Suppose in this section that $G_K(2) \simeq G_{\mathbb{Q}_2}(2)$ and $k = K \cap \overline{\mathbb{Q}}$ satisfies the conditions of Case B in Lemma 3.9. Then k admits an ordering as well as a p-adic valuation v_p where $p \equiv 5\,(8)$. Furthermore, $k^\times/(k^\times)^2$ admits an $\mathbb{F}_2$-basis $\langle -1, 2, c\rangle$, where $v_p(c) > 0$ is odd. It is also straightforward now to work out the structure of the norm groups. Indeed, since we know that $N_k(-1) = \langle 2, c\rangle$, reciprocity quickly gives us $N_k(2), N_k(c)$ and $N_k(2c)$. Note that $G_k(2)$ is not Demushkin, so we cannot have $-c \in N_k(-2)$. Indeed, otherwise $N_k(-2) = \langle 2, c\rangle$, from which we quickly obtain $N_k(-c) = \langle -2, c\rangle$

and $N_k(-2c) = \langle -c, 2c\rangle$. Since all the norm groups then have index 2, Proposition 2.10 implies that $G_k(2)$ would be Demushkin.

In conclusion we get the following 'lattice':

- $N_k(-1) = \langle 2, c\rangle$
- $N_k(2) = \langle -1, 2\rangle$
- $N_k(c) = \langle -1, c\rangle$
- $N_k(2c) = \langle -1, 2c\rangle$
- $N_k(-2) = \langle 2\rangle$
- $N_k(-c) = \langle c\rangle$
- $N_k(-2c) = \langle 2c\rangle$

The 'lattice' for K is the same except $N_K(-2) = \langle 2, -c\rangle$, $N_K(-c) = \langle c, -2\rangle$ and $N_K(-2c) = \langle 2c, -2\rangle$

Since 2 is a square in the real closure of k but not in k, we must have that $2 \notin (k^h)^2$ and so, by henselianity, $2 \notin (k^h v_p)^2$. Thus $k^h(\sqrt{2})$ is the unique unramified extension of k^h, and so $\mathcal{O}(N_k(2))$ defines the p-adic valuation ring in k^h, and hence also in k. The goal now is to derive a contradiction from the following

Proposition 4.17. *If k is as described above, then $\mathcal{O}(N_K(2))$ defines a (non-trivial) valuation v on K with Kv not 2-closed.*

Indeed, taking this as given for the present, this valuation on K will not have 2-divisible value group, by virtue of the fact that $c \notin N(2)$. Hence the same is true for K^h, the 2-henselization of K, and the residue field is again not 2-closed. In other words, K^h admits a 2-henselian valuation tamely branching at 2. Then $G_{K^h}(2) \simeq \mathbb{Z}_l \rtimes \mathbb{Z}_l$ where l is the residue characteristic. By [7] Theorem 2.15, it follows that $\mathbb{Q}_2$ admits a (non-2-henselian) valuation w tamely branching at 2: in particular w has non-2-closed residue field. The henselization $\mathbb{Q}_2^w$ with respect to w therefore admits two henselian valuations, namely w and the duadic valuation. Since these have different residue characteristic they are incomparable. By F.K. Schmidt's Theorem (Theorem 4.4.1 in [3]) $\mathbb{Q}_2^w$ is algebraically closed, contradicting the fact that $\mathbb{Q}_2^w w$ is not 2-closed.

All that remains is to prove Proposition 4.17. We will do so using the same techniques as in Case A. The fact that we are working with an undetermined 'c' rather than the simple integer 5 might appear to make this a gruelling task. However, a closer inspection of the calculations in Case A show that the crucial information needed was the square values of $3, c-1, c-2, c-3$ and $c-4$. In Case A these were all easy to determine, and it turns out that any c such that $c-1 \sim 1, c-2 \sim -c, c-3 \sim 2, c-4 \sim 1$ would do in place of 5. In our present case, once we fix the value of 3, we can work out the rest of the values. Since $3 \in N_k(-2) = \langle 2 \rangle$, we have $3 \sim 1$ or $3 \sim 2$. It would be desirable to have a proof as in Lemma 3.3 which shows 3 is not a square, but while we suspect it may be possible to do so by considering dihedral extensions of $\mathbb{Q}_2$ of order 8, we have been unable to find such an argument. Instead both cases are considered separately.

The computations proceed the same way in both cases. First one shows by direct computation that whether $3 \sim 1$ or 2, we always have $\pm 1, \pm 2, \pm 1/2 \in \mathcal{O}_2$. This allows us to compile a list of the possible square classes of expressions $1 + ax$, where $a \in \{\pm 1, \pm 2, \pm 1/2\}$, $x \in \mathcal{O}_1$. This list turns out to be independent of the square class of 3. Finally, one uses this list to check that $1 - xy \in N(2)$ for any $x, y \in \mathcal{O}_1$, thereby completing the proof by Lemma 4.1. The details can all be found in Appendix C.

5 The Birational Section Conjecture

We conclude with an application to the birational section conjecture (see [8] for background details). Recall that given a smooth, complete curve X over a field K, there is a canonical exact sequence of Galois groups

$$1 \to G_{\overline{K}(X)} \to G_{K(X)} \to G_K \to 1 \tag{8}$$

where $K(X)$ is the function field of X and $\overline{K}(X) = \overline{K} \otimes_K K(X)$.

Given any $a \in X(K)$, we can assign to it a 'bouquet' of group-theoretic sections $s_a : G_K \to G_{K(X)}$. Indeed, let v_a be the valuation on $K(X)$ corresponding to a, and w the valuation on $\overline{K}(X)$ corresponding to a preimage of a in $\overline{X} := X \otimes_K \overline{K}$ (so w extends v). If we let I_w and D_w denote the inertia and decomposition group of w/v inside $G_{K(X)}$, then we get by Hilbert Decomposition Theory a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_{\overline{K}(X)} & \longrightarrow & G_{K(X)} & \longrightarrow & G_K & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow \simeq & & \\ 1 & \longrightarrow & I_w & \longrightarrow & D_w & \longrightarrow & G_w & \longrightarrow & 1 \end{array}$$

with exact rows. Here G_w denotes the Galois group of the residue field extension. It is known that the bottom row admits sections (see e.g. [9]). Any choice of such induces a section s_w of (8) such that $s(G_K) \subset D_w$, which is unique up to conjugation by an element of $G_{\overline{K}(X)}$. Any member of the 'bouquet' of sections obtained in this manner is said to lie over a. In a similar manner, if v is a valuation which is trivial on K and has residue field K, the same discussion shows that v induces a 'bouquet' of sections which are said to lie over v. We call such valuations **K-valuations**.

The *birational anabelian section conjecture* of Grothendieck says that *every* section of (8) lies over a unique $a \in X(K)$. This was proved in [8] in the case where K is a finite extension of $\mathbb{Q}_p$. Pop later showed in [15] that one could obtain a bijection already by considering a much smaller quotient of (8), the maximal $\mathbb{Z}/p\mathbb{Z}$ elementary meta-abelian quotient. Conjecture 1 implies that if the groundfield contains ζ_p, then one obtains a bijection when considering the maximal pro-p quotient. This already follows from Pop's Theorem, but the proof we give is independent.

We also note that the generality of our main theorem means we can prove a statement for varieties, not just curves. The pendant for the birational section conjecture in higher dimensions was proven by Stix in [21]. Here one finds that every section lies over a unique K-valuation. When X is a curve, it is well known that such valuations correspond exactly to points. For higher dimensions, such valuations always imply the *existence* of a point, but the valuation itself need not be induced by this point. That is, non-geometric sections exist. In [16], Pop generalized this again to the metabelian setting, but only in the case when $p > 2$. Our main result allows us to partially fill this gap.

Proposition 5.1. *Assume Conjecture 1 holds, and suppose X is a smooth, projective variety over F of dimension n, where F is a finite extension of $\mathbb{Q}_p$ containing ζ_p. Then given any section s of*

$$1 \to G_{\overline{F}(X)}(p) \to G_{F(X)}(p) \to G_F(p) \to 1$$

there is a finite extension F' of $\mathbb{Q}_p$ containing ζ_p such that $G_{F'}(p) \simeq G_F(p)$ and $s'(G_{F'}(p)) \subset D_{w'}$ for a unique F'-valuation w'. Here $s' : G_{F'}(p) \to G_{F'(X)}(p)$ is the section induced by s.

Proof. Let $s : G_F(p) \to G_{F(X)}(p)$ be a section, and let K be the fixed field in $F(X)(p)$ of $s(G_F(p))$. Then $G_K(p) \simeq s(G_F(p)) \simeq G_F(p)$. By Conjecture 1, there is a finite extension $F'/\mathbb{Q}_p$ and a valuation v on K satisfying the properties of the Conjecture. In particular, the residue field is finite and $v(\pi)$ is a minimal positive element in Γ_v, where π is a uniformizer in F'. Then the restriction w of v to $F'(X)$ still has residue field $F'v$ and $w(\pi)$ is a minimal positive element.

Consider the subgroup H of Γ_w generated by $w(\pi)$. It is a convex subgroup isomorphic to $\mathbb{Z}$. Since F' is complete, it admits no immediate extensions of transcendence degree n. Therefore $H \neq \Gamma_w$. Let w' be the valuation obtained from w with value group Γ_w/H. By construction, w' is trivial on F' and has residue field F', since $w'(\pi) = 0$. Since w' is a coarsening of a p-henselian valuation, it is itself p-henselian. Hence w' is an F'-valuation with $s(G_F(p)) \subset D_{w'}$.

To show uniqueness, suppose w'' is another valuation such that $s(G_{F'}(p)) \subset D_{w''}$. Then as both are p-henselian with residue field not p-closed, they are either independent or comparable, by general valuation theory. The p-version of F.K. Schmidt's Theorem implies that they are not independent, and so they must be comparable. If w' is a coarsening of w'', then the quotient valuation w''/w' is a p-henselian valuation on an algebraic extension of F' with residue field F', and hence must be trivial. That is, $w'' = w'$. The argument is identical if w'' is a coarsening of w'. □

Remark 5.2. By Remark 2.9, if $F = \mathbb{Q}_p(\zeta_p)$, then $F' = F$ in the statement of the above.

Corollary 5.3. *Assume Conjecture 1 holds, and suppose X is a smooth, projective variety over F, where F is a finite extension of $\mathbb{Q}_p$ containing ζ_p. Then there is a section of (8) if and only if $X(F) \neq \emptyset$.*

Proof. Note that the valuation w' of Proposition 5.1 defines an F'-rational place of $F(X)$, and hence gives rise to a point in $X(F')$. Indeed, we may always choose a generic point in $F(X)$ with positive value. Its image under the place gives a rational point $a \in X(F')$. Since the restriction map $G_K(p) \to G_F(p)$ is an isomorphism, F is relatively algebraically closed in K, and because X is defined over F, in fact $a \in X(F)$, as desired. □

Corollary 5.4. *Assume Conjecture 1 holds, and suppose X is a smooth, projective* curve *over F, where F is a finite extension of $\mathbb{Q}_p$ containing ζ_p. Then every section of (8) lies over a unique F-rational point $a \in X(F)$.*

Proof. This follows from the above corollary at once using Lemma 1.7 from [8]. Alternatively, it is a classical result that for curves, all K-valuations come from K-rational points. □

The main theorem therefore yields the following unconditional result:

Corollary 5.5. *Suppose X is a smooth, complete variety over $\mathbb{Q}_2$. Then any group-theoretic section of the exact sequence*

$$1 \to G_{\overline{\mathbb{Q}_2(X)}}(2) \to G_{\mathbb{Q}_2(X)}(2) \to G_{\mathbb{Q}_2}(2) \to 1$$

lies above a unique $\mathbb{Q}_2$-valuation v, which corresponds to a $\mathbb{Q}_2$-rational point if X is a curve. In both cases, the existence of a section implies that $X(\mathbb{Q}_2) \neq \emptyset$.

Using Corollary 4.16, we even obtain the same conclusion using just the maximal $\mathbb{Z}/2\mathbb{Z}$ elementary meta-abelian quotients.

6 Appendix

We detail the missing calculations.

A. Case A

Let us begin by proving Lemma 4.4. We want to show that for $x \in \mathcal{O}_1$, $1+2x$ and $1+4x$ are in $N(5)$.

Remark 6.1. Let us emphasize that in the calculations below, the *order* in which calculations are done is crucial.

Proof. We proceed by cases, based on the square classes of x and $1+x$. We write $x \sim y$ to denote that x and y have the same square class, i.e., x/y is a square in K. Throughout we use freely Proposition 3.10 to determine intersections of various norm groups.

Note also that $x \in \mathcal{O}_1$ implies $x \sim \pm 2, \pm 10$. If $x \sim 2$, then $1+x \in N(5) \cap N(-2) = \{1, -5\}$, and similarly when $x \sim -2$ or ± 10. Therefore the cases considered below are indeed exhaustive.

- $\boxed{x \sim 2, 1+x \sim 1}$ Note that $1+2x = (1+x)+x \in N(-1) \cap N(-2) = \{1, 2\}$. Also we have $1+5x = (1+x)+4x \in N(-10) \cap N(-2) = \{1, -5\}$. If $1+5x \sim -5$, with say $1+5x = -5a^2$, then one finds $1+2x = (1+5x) - 3x \in -5N(2) = \{\pm 5, \pm 10\}$, contradiction.

  Hence $1+5x \sim 1$ whence $1+2x = (1+5x)-3x \in N(-10)$, so $1+2x \sim 1$. Now $1+4x = (1+x)+3x \in N(-2) \cap N(-10) = \{1, -5\} \subset N(5)$.

- $\boxed{x \sim 2, 1+x \sim -5}$ Then $1+2x \in N(-1)$, and, equalling $(1+x)+x$ can be written in the form $-5a^2+2b^2$ for some a and b, or equivalently $-5(A^2-10B^2)$ for some A, B. This expression is visibly in $-5N(10)$, and so $1+2x \in N(-1) \cap -5N(10) = \{2, 5\}$. Suppose for a contradiction that $1+2x \sim 2$. Then $1+3x = (1+x)+2x = (1+2x)+x \in N(10) \cap N(5) \cap N(-1) = \{1\}$, so $1+3x \sim 1$. Therefore $1+5x = (1+x)+4x = (1+3x)+2x \in N(-10) \cap 2N(10) \cap N(-1) = \varnothing$: contradiction. Hence $1+2x \sim 5$, and also $1+5x = (1+x)+4x = (1+2x)+3x \in N(-10) \cap 2N(10) \cap 5N(2) = \{-5\}$, so $1+5x \sim -5$.

  From this we get $1+4x = (1+2x)+2x = (1+5x)-x \in N(-2) \cap N(-5) \cap N(-10) = \{1\}$, so $1+4x \sim 1$.

- $\boxed{x \sim -2, 1+x \sim 1}$ We have $1-4x = (1+x)-5x \in N(-2) \cap N(-10) = \{1, -5\}$. Also $1-x = (1+x)-2x \in N(-2) \cap N(-1) = \{1, 2\}$. If $1-x \sim 2$ then we get $1-4x = (1-x)-3x \in 2N(5)$, giving a contradiction. So $1-x \sim 1$. Hence $1+4x = (1-x)+5x = (1+x)+3x \in N(2) \cap N(10) \cap N(-10) = \{1\}$.

  Next, $1+2x = (1+4x)-2x = (1+x)+x = (1-x)+3x \in N(-1) \cap N(2) \cap N(-10) = \{1\}$.

- $\boxed{x \sim -2, 1+x \sim -1}$ Then $1+4x = (1+x)+3x \in N(2) \cap N(10) = \{1, -1\}$.

  Now, $1-5x = (1+x)-6x \in N(-10) \cap -N(-5) = \{-5, 10\}$. If $1+4x \sim -1$, then also $1-5x = (1+4x)-9x \in N(2)$ as well, giving a contradiction as neither -5 or 10 are in $N(2)$. Thus $1+4x \sim 1$, whence $1+5x = (1+x)+4x = (1+4x)+x \in N(10) \cap -N(-2) \cap N(2) = \{-1\}$.

  From this we get that $1+2x = (1+x)+x = (1+4x)-2x = (1+5x)-3x \in -N(-2) \cap N(-1) \cap -N(-10) = \{5\}$.

- $\boxed{x \sim 10, 1+x \sim 1}$ First note $1-2x \in N(5) \cap N(-2) = \{1, -5\}$. Also, $1-x \in N(10) \cap N(5) = \{1, -1\}$. If $1-x \sim -1$, then $1-2x = (1-x)-x \in -N(-10)$, a contradiction. Therefore $1-x \sim 1$.

  Now, $1+2x \in N(-5) \cap N(-10) = \{1, -2\}$. Suppose $1+2x \sim -2$. Then $1+3x = (1+x)+2x = (1+2x)+x \in N(2) \cap N(-5) \cap 2N(5)$ giving $1+3x \sim 2$. Then $1+4x \in N(-10) \cap N(2) \cap 2N(5)$ giving $1+4x \sim -2$. Finally, this gives $1-x = (1+4x)-5x \in -N(-1)$, a contradiction.

  Hence $1+2x \sim 1$. The above also shows $1+4x$ is not equivalent to -2. But $1+4x \in N(-10) \cap N(2)$, so $1+4x \sim 1$.

- $\boxed{x \sim 10, 1+x \sim -5}$ We have $1+2x \in N(-5) \cap 5N(2) = \{5, -10\}$. Assume, for a contradiction, that $1+2x \sim -10$.

  Then $1-x = (1+2x)-3x = (1+x)-2x \in 2N(5) \cap N(10) \cap -N(-1) = \{-10\}$. Now, $1+4x = (1+2x)+2x \in 5N(2) \cap N(-10) = \{-5, 10\}$. Next, $1-4x = (1+x)-5x = (1-x)-3x \in N(10) \cap -5N(-10) \cap 2N(5) = \{10\}$. Thus $1+4x = (1-4x)+8x \in 5N(-2)$, whence $1+4x \sim 10$. This in turn forces $1+5x = (1+4x)+x \sim N(-1)$. But also $1+5x = (1+x)+4x \in N(-2) \cap 5N(2)$, which has empty intersection with $N(-1)$. So we get our required contradiction.

Therefore $1+2x \sim 5$. We also showed above that $1+4x \sim -5$ or 1, so we're again done in this case.

- $\boxed{x \sim -10, 1+x \sim 1}$: It is immediate that $1+2x \in N(5) \cap N(10) = \{1,-1\}$. Next, observe that $1+4x \in N(10) \cap N(-2) = \{1,-10\}$. But if $1+4x \sim -10$, we find $1+2x = (1+4x)-2x \in 5N(2)$, a contradiction to the above. Hence $1+4x \sim 1$ and we are done.

- $\boxed{x \sim -10, 1+x \sim -1}$ We have $1+2x \in N(5)$ at once, and $1+4x = (1+x)+3x \in N(2) \cap N(10) = \{1,-1\}$.

This completes the proof. □

Corollary 4.5 then shows that $\mathcal{O}_1$ is closed under multiplication by $\pm 1, \pm 5$ and $\pm 5^{-1}$. For the proof of the crucial Proposition 4.6, we will want to use more detailed knowledge of how multiplication of these numbers permutes the elements in $\mathcal{O}_1$. More specifically, given $x \in \mathcal{O}_1$, where we know the square class of x and $1+x$, we want to know the square class of ax and $1+ax$, for $a \in \{\pm 1, \pm 5, \pm 5^{-1}\}$. We proceed in a similar manner as the proof of Lemma 4.4: the idea is essentially to express $1+ax$ as a norm in two or three different ways. For example, if $x \sim 2, 1+x \sim 1$, then $1-5x = (1+x)-6x \in N(10) \cap N(-5) \cap N(5) = \{1\}$, so $1-5x$ is a square.

The other calculations are entirely similar and are left to the reader. We note also that the proof of Lemma 4.4 dealt already with a few cases. The results are summarized in Table 1 below.

Table 1: Stability of $\mathcal{O}_1$ under $N(5)$

x	$1+x$	$1-x$	$1+5x$	$1-5x$	$1+5^{-1}x$	$1-5^{-1}x$
2	1	1,-1	1	1	1	1
2	-5	-1	-5	± 1	-1,5	± 1
-2	1	1	± 1	1,-5	1	-1, 5
-2	-1	1, -5	-1	1,-5	± 5	-5
10	1	± 1	1,-5	1	1	1
10	-5	-1	-5	± 1	1,-5	1
-10	1	1,-5	± 1	1	1	1,-5
-10	-1	1,-5	± 1	1, -5	± 1	-5

Note that given the explicit information provided by the proof of Lemma 4.4, it is possible to make every entry unique in this table, and indeed even to

pin down the exact value of $1+ax$ for $a \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 5^{-1}, \pm 3^{-1}\}$. However, this will not be necessary to complete the remaining proofs; the table above will suffice.

Finally, we include all the remaining calculations of Proposition 4.6. That is, we systematically show that for all possible combinations of the square classes of $x, 1+x, y, 1+y$ with $x, y \in \mathcal{O}_1$, $1-xy \in N(5)$. Clearly if $x \sim 2, y \sim 10$ or $x \sim -2, y \sim -10$ then $1-xy \in N(5)$ is automatic. Next observe that any $x \in \mathcal{O}_1$ is of the form $2ab^2$ where $a \in \{\pm 1, \pm c\}$. Since for any such a and any other $y \in \mathcal{O}_1$, $ay \in \mathcal{O}_1$, we can without loss of generality always assume that $x \sim 2$. We also freely exploit symmetry in x and y to reduce the number of cases to those done below.

Let us recall that we have the decomposition

$$1 - xy = (1+ay)\left(1 + (1+ax)\frac{-ay}{1+ay}\right) \tag{9}$$

for $a = \pm 1, \pm 5$. We will refer to the decomposition with respect to a as the a-decomposition. So the -1-decomposition means

$$1 - xy = (1-y)\left(1 + (1-x)\frac{y}{1-y}\right)$$

We will use this freely in what follows. The calculations involved are trivial; the difficulty is in identifying which calculations will actually give the desired result. Therefore in the below, rather than include all the details of the arithmetic, we simply indicate how to proceed. Note we will also use without comment the result of Table 1 above.

Proof. (Proposition 4.6) By the above discussion, we only need to check the following cases:

- $\boxed{x \sim 2, 1+x \sim 1, y \sim 10, 1+y \sim 1}$ Immediate.
- $\boxed{x \sim 2, 1+x \sim 1, y \sim 10, 1+y \sim -5}$ Immediate.
- $\boxed{x \sim 2, 1+x \sim 1, y \sim -10, 1+y \sim 1}$ We immediately get $1-xy \in N(-5)$, and the $+1$-decomposition gives also $1-xy \in N(-10)$, so $1-xy \in \{1, -2\}$. Now $1+5^{-1}y \sim 1$. Also, $1+5x \sim 1$ or -5. But since $1-5x \sim 1$, we get $1+5x = (1-5x)+10x \in N(-5)$, so in fact $1+5x \sim 1$. Therefore the $+5$-decomposition gives $1-xy \in N(10)$, forcing $1-xy \sim 1$.

- $\boxed{x \sim 2, 1+x \sim 1, y \sim -10, 1+y \sim -1}$ We immediately get $1-xy \in N(-5)$, and the $+1$-decomposition also gives $1-xy \in N(-2)$. So $1-xy \in \{1,-10\}$. Also, $1-5^{-1}y \sim -5$ and $1-5x \sim 1$, whence the -5-decomposition gives $1-xy \in N(2)$, forcing $1-xy \sim 1$.

- $\boxed{x \sim 2, 1+x \sim -5, y \sim 10, 1+y \sim 1}$ Immediate.

- $\boxed{x \sim 2, 1+x \sim -5, y \sim 10, 1+y \sim -5}$ Immediate.

- $\boxed{x \sim 2, 1+x \sim -5, y \sim -10, 1+y \sim 1}$ We immediately get $1-xy \in N(-5)$, and the $+1$-decomposition gives $1-xy \in N(2)$. We also see $1-5y \sim 1$. Since $1-x \sim -1$, we find $5-x \in -N(-1)$, and since $1-5^{-1}x \sim \pm 1$, we get $1-5^{-1}x \sim -1$. Using the -5-decomposition now gives $1-xy \in N(-2)$, forcing $1-xy \sim 1$.

- $\boxed{x \sim 2, 1+x \sim -5, y \sim -10, 1+y \sim -1}$ We immediately get $1-xy \in N(-5)$, and $1-xy = (1+y)(1+(1+x)\frac{-y}{1+y})$ gives $1-xy \in \{-2,5\}$. Now $1-5^{-1}y \sim -5$ forces $1-y \sim -5$. So using $1-xy = 1-xy = (1-y)(1+(1-x)\frac{y}{1-y})$ quickly gives $1-xy \sim 5$.

- $\boxed{x \sim 2, 1+x \sim 1, y \sim 2, 1+y \sim 1}$ The $+1$-decomposition yields $1-xy \in N(2)$. Now $1-x \sim 1, 1-y \sim 1$, so the -1-decomposition yields $1-xy \in N(-2)$. Hence $1-xy \in \{1,2\}$. Also, $1-5y \sim 1, 1-5^{-1}x \sim 1$, so the -5-decomposition gives $1-xy \in N(-10)$ forcing $1-xy \sim 1$.

- $\boxed{x \sim 2, 1+x \sim 1, y \sim 2, 1+y \sim -5}$ The $+1$-decomposition gives $1-xy \in N(-10)$. Also, $1-xy \sim 1, 1-y \sim 1$ so the -1-decomposition yields $1-xy \sim 1, -5$.

- $\boxed{x \sim 2, 1+x \sim 1, y \sim -2, 1+y \sim 1}$ The $+1$-decomposition gives $1-xy \in N(-2) \cap N(2) = \{1,2\}$. Also, $1+5x \sim 1, 1+5^{-1}y \sim 1$, so the $+5$-decomposition gives $1-xy \in N(10)$ whence $1-xy \sim 1$.

- $\boxed{x \sim 2, 1+x \sim 1, y \sim -2, 1+y \sim -1}$: We immediately get $1-xy \in N(-1)$, and the $+1$-decomposition gives $1-xy \in -N(2)$, so $1-xy \in \{1,2\}$. Also, $1+5y \sim -1, 1+5^{-1}x \sim 1$, so the $+5$-decomposition gives $1-xy \in N(10)$, forcing $1-xy \sim 1$.

- $\boxed{x \sim 2, 1+x \sim -5, y \sim 2, 1+y \sim -5}$ The $+1$-decomposition gives $1-xy \in -5N(2)$. Also, $1-x \sim -1, 1-y \sim -1$, so the -1-decomposition gives $1-xy \in -N(-2)$, forcing $1-xy \in \{5, 10\}$. Finally, the -5-decomposition gives $1-xy \in -N(-10)$ which gives $1-xy \sim 5$.

- $\boxed{x \sim 2, 1+x \sim -5, y \sim -2, 1+y \sim 1}$ We immediately get $1-xy \in N(-1)$. The $+1$-decomposition gives $1-xy \in N(-10)$ so $1-xy \in \{1, 10\}$. Also, $1-xy \sim -1, 1-y \sim 1$ so the $+1$-decomposition gives $1-xy \in N(-2)$, forcing $1-xy \sim 1$.

- $\boxed{x \sim 2, 1+x \sim -5, y \sim -2, 1+y \sim -1}$ We immediately get $1-xy \in N(-1)$. The $+1$-decomposition gives $1-xy \in N(-10) \cap -N(-1)$, so $1-xy \in \{2, 5\}$. Also, $1-5x \sim -1$ and $1-5^{-1}y \sim -5$, whence the -5-decomposition gives $1-xy \in -N(-2)$, forcing $1-xy \sim 5$.

In all cases $1-xy \in N(5)$, completing the proof. □

B. Calculation of the Residue Field in Case A

We complete the proof of Proposition 4.13. As remarked there, it suffices to show in all cases either that $1+x \notin N(5)$, or that $3+x \notin N(5)$; the former implies $1+x \in \mathcal{O}_1$, while the latter implies $1+x \in 2\mathcal{O}_1$.

Lemma 6.2. *If $x \in \mathcal{O}^\times, x \sim -1$, then $3+x \notin N(5)$.*

Proof. By assumption, and Corollary 4.10, $1+2x \in N(5)$. We have $1+2x \in N(5) \cap N(2) = \{\pm 1\}$. Suppose $1+2x \sim 1$, with $1+2x = a^2$ say. Then $2+x = a^2/2 + 3/2 = 2A^2 - 10B^2$ for some A, B. Hence $1+2x \in 2N(5)$, a contradiction. Thus $1+2x \sim -1$.

Write $1+2x = -a^2$ for some a. Then $2+x \in N(-5)$ by a calculation identical to the above. Also $2+x \in N(2)$ is immediate, while by Corollary 4.10, $2+x \in N(5)$ as well, forcing $2+x \sim 1$. Thus $3+x \in -N(-5) \cap N(-1) = \{2, 10\}$. □

Lemma 6.3. *If $x \in \mathcal{O}^\times, x \sim 5$, then $1+x \notin N(5)$.*

Proof. $1+2x \in N(5) \cap N(-10) = \{1, -5\}$. If $1+2x \sim 1$, say equalling a^2, then we find $2+x \in 2N(5)$ as in the above lemma. Therefore we must have $1+2x \sim -5$. Again using Corollary 4.10, $2+x \in -N(-1) \cap N(5) = \{-1, -5\}$.

Also, $2 + x = 2 + 5b^2$ for some b, which can't be -5 modulo squares, since $2 \notin -N(-1)$. Hence $2 + x \sim -1$.

If $1 + x \in N(5) \cap N(-5) = \{1, 5\}$, then $1 + x \sim 1$ gives $2 + x \in N(-1)$, contradiction. Similarly, $1 + x \sim 5$ gives $2 + x \in N(-5)$, contradiction.

Hence $1 + x \notin N(5)$. □

Lemma 6.4. *If $x \in \mathcal{O}^\times, x \sim -5$, then $3 + x \notin N(5)$.*

Proof. $1 + 2x \in N(5) \cap N(10) = \{\pm 1\}$. As in the proofs of the above cases, $1+2x$ is not a square, so $1+2x \sim -1$, giving $2+x \in N(-5) \cap N(5) = \{1, 5\}$. Also, $2+x = 2-5b^2$ for some b, which gives $2+x \sim 5$. Thus $3+x \in N(-5)$.

But in addition, $3 + x \in -N(-1)$ is visible, so $3 + x \in \{-2, -10\}$, as desired. □

This completes all the cases, and hence the proof that $Kv \simeq \mathbb{F}_2$.

C. Case B

As explained, the calculations depend on whether $3 \sim 1$ or $3 \sim 2$. Suppose that $3 \sim 2$. Let v_p denote the p-adic valuation on k. Then $v_p(c - 2) = v_p(2) = 0$, since $v_p(c) > 0$. Hence $c - 2 \in N_k(2)$. It's easy to rule out ± 1 as possibilities, using that $c \notin N(2) \cup N(-2)$. Hence $c - 2 \sim \pm 2$. Since $(k, <)$ is archimedean, we can always multiply c by a^2 where $1 < a^2 < 2$, and still have $c - 1 \sim 1$ (and so $c \in N_k(-1)$). By choosing a suitable such a^2, we can force $a^2c - 2$ to be negative, and hence we may without loss of generality assume that $c - 2 \sim -2$. From here it is easy to pin down the value of $c - 3$ and $c - 4$, and a similar argument deals with the case when $3 \sim 1$. The result is summarized in the following table:

Table 2:

3	$c-2$	$c-3$	$c-4$
2	-2	-2	-1
1	-2	-1	-1

Note that by our choice of c, we always have $c - 1 \sim 1$.

Lemma 6.5. *Suppose $3 \sim 2$. Then $-1, 2$ and $1/2 \in \mathcal{O}_2$, and consequently so is -2 and $-1/2$.*

Proof. Pick $x \in \mathcal{O}_1$. We have to show that also $-x, 2x$ and $x/2 \in \mathcal{O}_1$. We proceed as always on a case by case basis. Our strategy is to do the calculations in full for the case when $x \sim c$, and then transfer most of the other cases back to this case.

- $\boxed{x \sim c, 1+x \sim -2}$ We have $1-x = (1+x)-2x \in N(c) \cap N(-2c) = \{1, -c\}$. Suppose, for a contradiction, that $1-x \sim -c$. Then $1+(c-1)x = (1-x)+cx \in N(-c) \cap N(c) = \{1, c\}$. Also, $1-(c-1)x = (1+x)-cx \in N(2c) \cap -N(-2) = \{-1, 2c\}$. If $1-(c-1)x \sim 2$, then we get $1+(c-1)x \in 2N(c) \cap \{1, c\} = \varnothing$. Hence $1-(c-1)x \sim -1$, which quickly implies that $1+(c-1)x \sim 1$, using that $1+(c-1)x = (1-(c-1)x)+2(c-1)x$. From here we get that $1+(c-2)x = (1+(c-1)x)-x = (1+x)+(c-3)x \in N(c) \cap N(2c) \cap N(-c) = \{1\}$. It is easy to check that $1+2x \sim -c$, whence $1-(c-2)x = (1+2x)-cx = (1+x)-(c-1)x = (1-(c-1)x)+x$ giving $1-(c-2)x \sim -c$. Putting $1-(c-2)x = -ca^2$ for some a, we get $2+ca^2 = 1+(c-2)x \sim 1$, whence $2 \in N(c)$: contradiction.

  Hence $1-x \sim 1$, from which we quickly find $1-2x = (1-x)-x = (1+x)-3x \in N(2c) \cap N(c) \cap N(-c) = \{1\}$. Finally, $1+2x = (1+x)+x = (1-2x)+4x \in N(-2c) \cap 2N(2c) \cap N(-c) = \{-2\}$. Checking that $2+x \in N(2)$ is straightforward.

- $\boxed{x \sim c, 1+x \sim 1}$ This case requires only the obvious calculations. For example, $1-x = (1+x)-2x \in N(c) \cap N(2c) = \{1, -1\} \subset N(2)$.

- $\boxed{x \sim -c, 1+x \sim 1}$ We have $1-x = (1+x)-2x \in N(-c) \cap N(-2c) = \{1, -2\} \subset N(2)$. Thus $-x \in \mathcal{O}_1$, and $-x \sim c$. But we know then from the above cases that $-2x, -x/2 \in \mathcal{O}_1$ as well, which gives us what we want.

- $\boxed{x \sim -c, 1+x \sim -1}$ We have $1-x = (1+x)-2x \in N(-c) \cap N(2c) = \{1, -2c\}$. Suppose, for a contradiction, that $1 = x \sim -2c$. Then $1+2x \in N(2c) \cap -N(-c) \cap -N(-1) = \{-1\}$. Next, $1-2x = (1+x)-3x = (1-x)-x \in N(-2c) \cap N(2c) \cap -N(-c) = \{2c\}$. It follows that $1-(c-3)x = (1+2x)-(c-1)x = (1+x)-(c-2)x = (1-x)-(c-4)x \in N(2c) \cap N(c) \cap -N(-2c) \cap N(-2) = \varnothing$.

  Hence we must have $1-x \sim 1$. In other words, $-x \in \mathcal{O}_1$. The other identities to check now follow at once as in the above case.

- $\boxed{x \sim 2c, 1+x \sim 1}$ We have $1-x = (1+x)-2x \in \{1,-1\}$. Next, $1+2x = (1+x)+x \in N(-c) \cap N(-2c) = \{1,-2\} \subset N(2)$. Finally, $2+x = 1+(1+x) \in -N(-c) \cap N(-1) = \{2, 2c\}$. If $2+x = 2cb^2$ for some b, then $1-x = 3-2cb^2 \in 2N(c) \cap \{1,-1\} = \varnothing$: contradiction. Hence $2+x \sim 2$.

- $\boxed{x \sim 2c, 1+x \sim -2}$ It's easy to check that $2+x \in N(2)$, hence $x/2 \in \mathcal{O}_1$. Since $x/2 \sim c$, we immediately get the other calculations for free.

- $\boxed{x \sim -2c, 1+x \sim 1}$ We have $1-x = (1+x)-2x \in N(-2c) \cap N(-c) = \{1,-2\}$. Hence $-x \in \mathcal{O}_1$, and $-x \sim 2c$. Thus we immediately deduce the remaining calculations from the above cases.

- $\boxed{x \sim -2c, 1+x \sim -1}$ We have $1-x = (1+x)-2x \in N(-2c) \cap N(c) = \{1,-c\}$. Suppose $1-x \sim -c$. Then we find $1+2x = (1+x)+x = (1-x)+3x \in N(c) \cap -N(-2c) \cap -N(-1) = \{-1\}$. Also, $1-2x = (1+x)-3x = (1-x)-x = (1+2x)-4x \in N(-c) \cap N(c) \cap cN(2) \in N(2c) = \varnothing$: contradiction. Hence $1-x \sim 1$ and so $-x \in \mathcal{O}_1$. As before, the rest of the calculations now follow from the above cases.

This completes all the cases and thereby the proof. □

Lemma 6.6. *Suppose* $3 \sim 1$. *Then* $-1, 2$ *and* $1/2 \in \mathcal{O}_2$, *and consequently so are* -2 *and* $-1/2$.

Proof. We will only do the case where $x \sim c$. All the other cases are easy to do by way of reducing to this case, as in the above lemma.

- $\boxed{x \sim c, 1+x \sim 1}$ It's easy to check that $1-x \in \{1,-1\}$. Next, $1+2x = (1+x)+x \in N(-2c) \cap N(-c) = \{1,-2\} \subset N(2)$. Finally, checking that $2+x \in N(2)$ is also easy.

- $\boxed{x \sim c, 1+x \sim -2}$ We find at once $1-x \in \{1,-c\}$. Suppose, for a contradiction, that $1-x \sim -c$. Then one shows in order that $1-2x \sim -2c$ and so $1+2x \sim -c$. Hence $1-(c-4)x = (1+2x)-(c-2)x = (1+x)-(c-3)x \in \{c\}$, whence $1-(c-2)x = (1+2x)-cx = (1+x)-(c-1)x = (1-(c-4)x)-2x \in \{2c\}$. But $1-(c-1)x \in \{1,-2\}$, and $(1-(c-2)x)-x \in cN(2) = \{\pm c, \pm 2c\}$: contradiction. Hence $1-x \sim 1$. It's now easy to check that $1+2x$ and $2+x$ are in $N(2)$.

□

Using only the obvious decompositions, along with the above lemmas, we can now easily compile the following table summarizing the relevant square classes:

Table 3: Stability of $\mathcal{O}_1$ under $N(2)$

x	$1+x$	$1-x$	$1+2x$	$1-2x$	$2+x$	$2-x$
c	1	1,-1	1	1,-1	2	2,-2
c	-2	1	-2	1	-1,2	2
-c	1	1,-2	1,-1	1,-2	2	-1, 2
-c	-1	1	-1	1	2,-2	2
2c	1	1,-1	1,-2	1,-1	2	2,-2
2c	-2	1	-2	1	1,-2	2
-2c	1	1,-2	1,-1	1,-2	2	-1,2
-2c	-1	1	-1	1	2,-2	2

Note that this table *does not depend on the square class of 3*. Our proof that $1-xy \in N(2)$ for $x, y \in \mathcal{O}_1$ will depend only on this table, hence completing the proof irrespective of the square class of 3. We use for this the following decompositions:

$$\begin{aligned} 1-xy &= (1+y)\left(1+(1+x)\frac{-y}{1+y}\right) \\ &= (1-y)\left(1+(1-x)\frac{y}{1-y}\right) \\ &= (1+2y)\left(1+(1+2^{-1}x)\frac{-2y}{1-2y}\right) \\ &= (1-2y)\left(1+(1-2^{-1}x)\frac{2y}{1-2y}\right) \end{aligned}$$

which we refer to respectively as the $+1, -1, +2$ and -2 decomposition (with respect to y; by symmetry we get analogous identities wrt. x). The following proposition now shows that $\mathcal{O}(N(2))$ does define a valuation ring.

Proposition 6.7. *If $x, y \in \mathcal{O}_1$, then $1-xy \in N(2)$.*

Proof. We once again can always assume that $x \sim c$. Thus we are left to check the following cases. We do the first case in full, and for the rest simply specify which decompositions to consider.

- $\boxed{x \sim c, 1+x \sim 1, y \sim c, 1+y \sim 1}$ We have $1-xy = (1+y)(1+(1+x)y')$ where $y' = \frac{-y}{1+y} \sim -c, 1+y' \sim 1$. Hence $1-xy \in N(c)$. Next, $1-xy = (1+2y)(1+(1+2^{-1}x)y'')$, where $y'' = \frac{-2y}{1+2y} \sim -2c, 1+y'' \sim 1$. Also, $1+2y \sim 1$ and $1+2^{-1}x \sim 1$ by Table 3. Hence this decomposition yields $1-xy \in N(2c)$, whence $1-xy \in \{1,-1\} \subset N(2)$ as desired.

- $\boxed{x \sim c, 1+x \sim 1, y \sim c, 1+y \sim -2}$ The $+1$-decomposition wrt. y gives $1-xy \in N(-2c)$, while the $+2$-decomposition wrt. y gives $1-xy \in N(-c)$. Hence $1-xy \in \{1,-2\} \subset N(2)$.

- $\boxed{x \sim c, 1+x \sim 1, y \sim -c, 1+y \sim 1}$ We immediately get $1-xy \in N(-c)$. The $+1$-decomposition wrt. y gives $1-xy \in N(-1)$, while the $+2$-decomposition wrt. x gives $1-xy \in N(2c)$. In total therefore $1-xy \sim 1$.

- $\boxed{x \sim c, 1+x \sim 1, y \sim -c, 1+y \sim -1}$ We immediately get $1-xy \in N(-c)$. The $+1$-decomposition wrt. x gives $1-xy \in N(-1)$, while the $+2$-decomposition wrt. y gives $1-xy \in N(2c)$. In total therefore $1-xy \sim 1$.

- $\boxed{x \sim c, 1+x \sim 1, y \sim 2c, 1+y \sim 1}$ This case is trivial.

- $\boxed{x \sim c, 1+x \sim 1, y \sim 2c, 1+y \sim -2}$ This case is trivial.

- $\boxed{x \sim c, 1+x \sim 1, y \sim -2c, 1+y \sim 1}$ We immediately get $1-xy \in N(-2)$. The $+1$-decomposition wrt. x gives $1-xy \in N(c)$, while the $+2$-decomposition wrt. x gives $1-xy \in N(2c)$. Hence $1-xy \sim 1$.

- $\boxed{x \sim c, 1+x \sim 1, y \sim -2c, 1+y \sim -1}$ Here the $+2$-decomposition wrt. x immediately gives $1-xy \in N(2)$.

- $\boxed{x \sim c, 1+x \sim -2, y \sim c, 1+y \sim -2}$ The $+1$-decomposition wrt. y gives $1-xy \in 2N(c)$, while the -1-decomposition wrt. y gives $1-xy \in N(-c)$. Finally, the -2-decomposition wrt. y gives $1-xy \in N(-2c)$, which gives in total that $1-xy \sim -2$.

- $\boxed{x \sim c, 1+x \sim -2, y \sim -c, 1+y \sim 1}$ We immediately get $1-xy \in N(-1)$. The $+1$-decomposition wrt. y gives $1-xy \in N(2c)$, while the $+2$-decomposition wrt. x gives $1-xy \in N(-c)$. In total therefore $1-xy \sim 1$.

- $\boxed{x \sim c, 1+x \sim -2, y \sim -c, 1+y \sim -1}$ We immediately get $1-xy \in N(-1)$. The $+1$-decomposition wrt. y gives $1-xy \in N(2c)$, while the -1-decomposition wrt. y gives $1-xy \in N(c)$. In total therefore $1-xy \sim 1$.

- $\boxed{x \sim c, 1+x \sim -2, y \sim -2c, 1+y \sim 1}$ We immediately get $1-xy \in N(-2)$. The $+1$-decomposition wrt. y gives $1-xy \in N(c)$, while the $+2$-decomposition wrt. x gives $1-xy \in N(-c)$. In total therefore $1-xy \sim 1$.

- $\boxed{x \sim c, 1+x \sim -2, y \sim -2c, 1+y \sim -1}$ The -1-decomposition wrt. y immediately gives $1-xy \in N(2)$.

For the last two cases, we have $x \sim c$ and $y \sim 2c$, whence $1-xy \in N(2)$ is immediate. □

It remains to show that the residue field is not 2-closed. In fact, we show that 2 is not a square in Kv. Since $2 \notin K^2$, it suffices to show that there is no $a \in \mathcal{O}$ such that $a^2-2 \in \mathcal{M}$, the maximal ideal. Therefore the following proposition finishes the proof that Case B cannot occur:

Proposition 6.8. *For any $a \in K$, we have that $(a^2-2)^{-1} \in \mathcal{O}_2$. Therefore if $a \in \mathcal{O}$, $a^2-2 \in \mathcal{O}^\times$.*

Proof. We need to show that for all $x \in \mathcal{O}_1$, $x/(a^2-2) \in \mathcal{O}_1$, which amounts to showing $1+\frac{x}{a^2-2} \in N(2)$, or equivalently, $a^2-(2-x) \in N(2)$. Since $\mathcal{O}_2$ is closed under multiplication by $\pm 1, \pm 2, \pm 1/2$, it suffices to check this when $x \sim c$. There are two cases to consider.

First suppose that $1+x \sim -2$. Then by Table 3, we see that $2-x \sim 2$, so clearly $a^2-(2-x) \in N(2)$.

Secondly suppose that $1+x \sim 1$. Then by Table 3, $1-x \sim \pm 1$. If $1-x \sim 1$, then it follows easily that $2-x \sim 2$ and we are done as above. Otherwise $1-x \sim -1$. In this case let $x' := -x$. Then $x' \sim -c$ and $1+x' \sim -1$. Again by Table 3 we find $2-x' \sim 2$. Hence we get $x'/(a^2-2) \in \mathcal{O}_1$, whence also $-x'/(a^2-2) = x/(a^2-2) \in \mathcal{O}_1$. □

References

[1] *I. Efrat*, Finitely generated pro-p Galois groups of p-Henselian fields, Journal of Pure and Applied Algebra **138** (1999), 215–228.

[2] *I. Efrat*, Demushkin fields with valuations, Math. Z. **243** (2003), 333–353.

[3] *A. Engler* and *A. Prestel*, Valued Fields, Springer-Verlag, 2005.

[4] *N. Frohn*, The Model Theory of Absolute Galois Groups, Ph.D. thesis, Freiburg University, 2011.

[5] *B. Jacob* and *R. Ware*, A recursive description of the maximal pro-2 Galois group via Witt rings, Math. Z. **200** (1989), 379–396.

[6] *J. Koenigsmann*, From p-rigid elements to valuations (with a Galois-characterization of p-adic fields), J. reine angew. Math **465** (1995), 165–182.

[7] *J. Koenigsmann*, Encoding valuations in absolute Galois groups, Fields Institute Communications **33** (2003), 107–132.

[8] *J. Koenigsmann*, On the section conjecture in anabelian geometry, J. reine angew. Math **588** (2005), 221–235.

[9] *F. Kuhlmann*, *M. Pank* and *P. Roquette*, Immediate and purely wild extensions of valued fields, Manuscr. Math. **55** (1986), 39–67.

[10] *T. Lam*, Introduction to Quadratic Forms over Fields, American Mathematical Society, 2005.

[11] *A. Merkurjev* and *A. Suslin*, K-cohomology of Brauer-Severi varieties and the norm residue isomorphism, Izv. Akad. Nauk SSSR, Ser. Mat. **46** (1983), 307–340.

[12] *S. Mochizuki*, A version of the Grothendieck conjecture for p-adic local fields, International Journal of Mathematics **6** (1997), 499–506.

[13] *J. Neukirch*, Algebraic Number Theory, Springer-Verlag, 1999.

[14] *F. Pop*, Galoische Kennzeichnung p-adisch abgeschlossener Körper, J. reine angew. Math. **392** (1988), 145–175.

[15] *F. Pop*, On the birational p-adic section conjecture, Compositio Math. **146** (2010), 621–637.

[16] *F. Pop*, $\mathbb{Z}/p$ metabelian birational p-adic section conjecture for varieties, Unpublished: available on authors website (2015).

[17] *A. Prestel* and *P. Roquette*, Formally p-adic fields, Springer-Verlag, 1980.

[18] *L. Ribes* and *P. Zalesskii*, Profinite Groups, Springer-Verlag, 2010.

[19] *J. Serre*, A Course in Arithmetic, Springer-Verlag, 1973.

[20] *J. Serre*, Galois Cohomology, Springer-Verlag, 2002.

[21] *J. Stix*, Birational p-adic Galois sections in higher dimensions, Israel Journal of Mathematics **198** (2013), 49–61.

J. Koenigsmann, Mathematical Institute, Oxford University, Oxford, OX2 6GG

E-mail address: koenigsmann@maths.ox.ac.uk

K. Strømmen, Mathematical Institute, Oxford University, Oxford, OX2 6GG

E-mail address: strommen@maths.ox.ac.uk